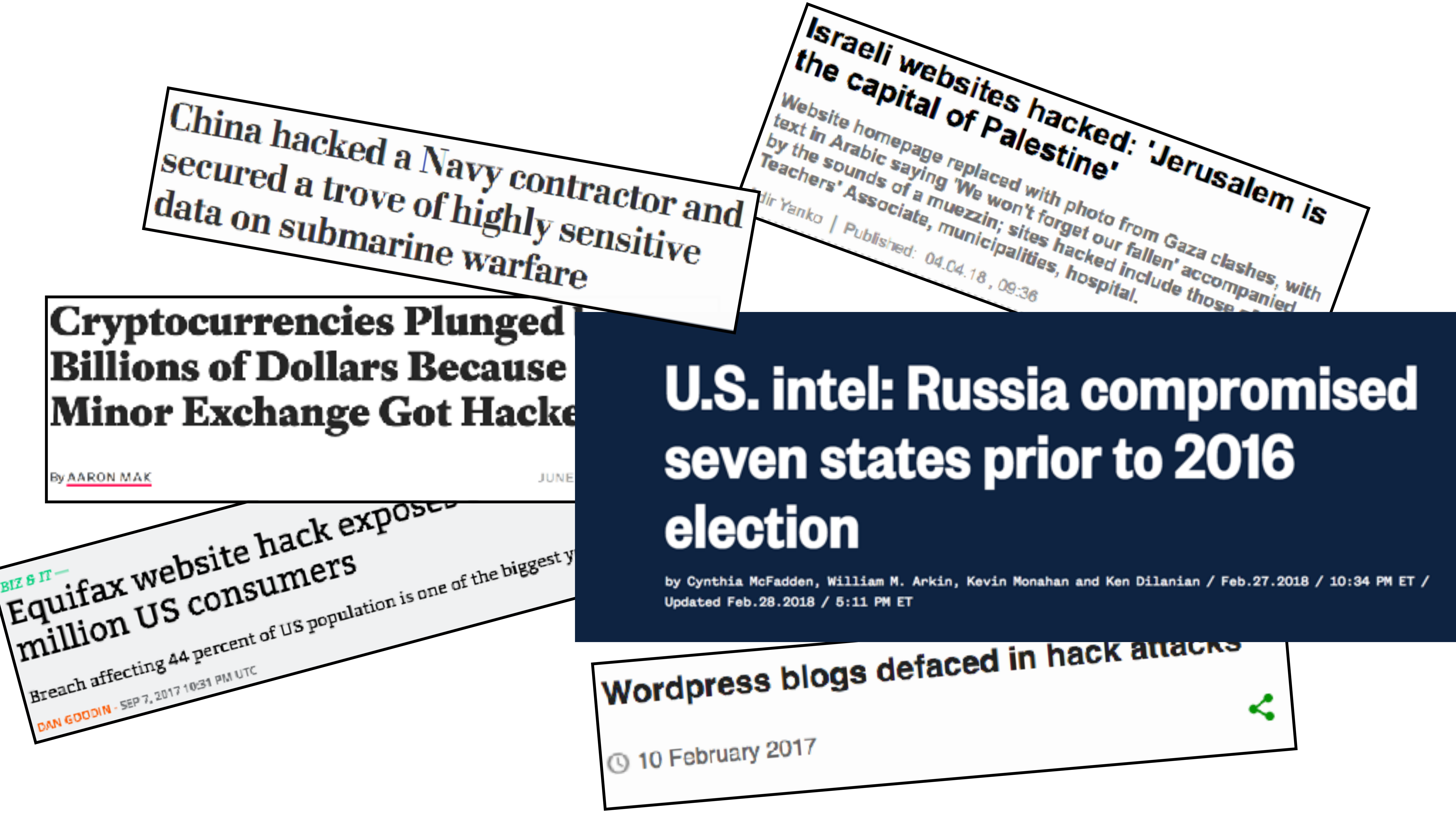
# What Can Governments Do About the Computer Security Crisis?

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

# We Have a Problem



China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare

Israeli websites hacked: 'Jerusalem is the capital of Palestine'

Website homepage replaced with photo from Gaza clashes, with text in Arabic saying 'We won't forget our fallen' accompanied by the sounds of a muezzin; sites hacked include those of Teachers' Associate, municipalities, hospital.

dir Yanko | Published: 04.04.18 , 09:36

Cryptocurrencies Plunged Billions of Dollars Because Minor Exchange Got Hacke

By AARON MAK JUNE

U.S. intel: Russia compromised seven states prior to 2016 election

by Cynthia McFadden, William M. Arkin, Kevin Monahan and Ken Dilanian / Feb.27.2018 / 10:34 PM ET / Updated Feb.28.2018 / 5:11 PM ET

BIZ & IT —

Equifax website hack expose million US consumers

Breach affecting 44 percent of US population is one of the biggest y

DAN GOODIN - SEP 7, 2017 10:31 PM UTC

Wordpress blogs defaced in hack attacks

10 February 2017

# We Have a Problem

- Our systems are constantly being hacked
  - Political motives, espionage, commercial motives, random vandalism
- Most sites can’t seem to stop the attackers
- Can governments help?

# Bad Ideas

- National firewalls
- Separating critical nets from the rest
- Authenticate everything

# National Firewalls?

- Countries are too big; even corporate firewalls are dicey these days
    - Besides, what about insiders (including visitors)
- It hurts innovation (do you block all new protocols or sites from your country) and hinders legitimate, necessary connectivity
- Totalitarian countries can approximate this—but even for them, it doesn’t work all that well

# The Military at Network Borders?

- Very intrusive; major privacy concerns
- Very inflexible—again, how do you deal with new protocols and required connectivity?
  - Firewalls enforce policies—what policy applies to an entire country?
- And what about encryption?

# Isolate Critical Networks?

- What is actually critical?
  - Can you keep the list up to date as things change?
- The critical and non-critical sectors need to talk to each other
  - Consumers do banking, everyone needs electricity, etc.
- The critical sectors rely on non-critical ones
  - Ordered-in food?

# Strongly Authenticate Everything?

- There are many indirect services, e.g., email and VoIP—whose identity do they carry?
  - Delegate your credentials to your email provider?
- When is a computer acting on behalf of a user and when is it autonomous?
- Attackers have long used “stepping stones”—and they’ll happily steal other folks’ credentials
  - The real problem is buggy code—and authentication code can also be buggy
- Besides, what about privacy?

# Many, Many More Bad Ideas

But what does work?

# Liability Disclaimers

- Apple: “YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, USE OF THE APPLE SOFTWARE AND ANY SERVICES PERFORMED BY OR ACCESSED THROUGH THE APPLE SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. [emphasis added]

- Microsoft: “you may not recover under this limited warranty, under any other part of this agreement, or under any theory, any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages. [emphasis added]

# Create Incentives

- Vendors have little incentive to prevent security problems—they've disclaimed responsibility

- Most security problems are caused by buggy code, but creating good code is expensive

    - (though the really big vendors do do a decent job)

- Governments should ensure that bad code is costly, too, by making sure that vendors of bad code are liable

    - In some situations, fines and penalties are also appropriate

# Insurance

- If there is liability, there will be insurance—but insurance companies need data
  - What is the frequency of hacks?
  - What was the root cause?
  - What defenses work? What doesn’t work?
- To get this data, security incidents have to be investigated, and the results published
  - This is why air travel is so safe—*all* accidents are investigated

# System Administration

- System administrators are the first line of defense against hackers
  - Most penetrations are due to exploitation of known, patchable holes
  - “At NSA we have not responded to an intrusion response that’s used a zero day vulnerability in over 24 months,” Hogue said. “The majority of incidents we see are a result of hardware and software updates that are not applying.” (David Hogue, NSA)
- Require disclosure of system administration quality to investors
- Take it into account when assessing fines and liability

# Encryption

- We need more of it

- “Exceptional access”—government back doors—will create insecurity

- (Research issue: how can keys be handled easily?)

# International Norms

- We don’t have strong international norms for cyberspace
- Is a government-sponsored hack an “armed attack”?
- Is espionage ok? Against commercial outfits?
- What about “preparing the battlefield”? Stepping stone attacks through third countries?

# It’s Not Easy!

- There are many complexities, objections, and exceptions to everything I’ve said

*But we have to start somewhere!*

# Questions?

(these slides at https://www.cs.columbia.edu/~smb/talks/cyberweek-gov_help.pdf)