

Why security (engineering)?

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts



A Ransomware Attack Has Struck a Major US Hospital Chain

"All computers are completely shut down," one Universal Health Services employee told WIRED.



Universal Health Services has 400 facilities across the US, Puerto Rico, and the UK. Its IT network has been down since Sunday. PHOTOGRAPH: GETTY IMAGES

UNIVERSAL HEALTH SERVICES, a hospital and health care network with more than 400 facilities across the United States, Puerto Rico, and United Kingdom, suffered a ransomware attack early Sunday morning that has taken down its digital networks at locations around the US. As the situation has spiraled, some patients have reportedly been rerouted to other emergency rooms and facilities and had appointments and test results delayed as a result of the attack.

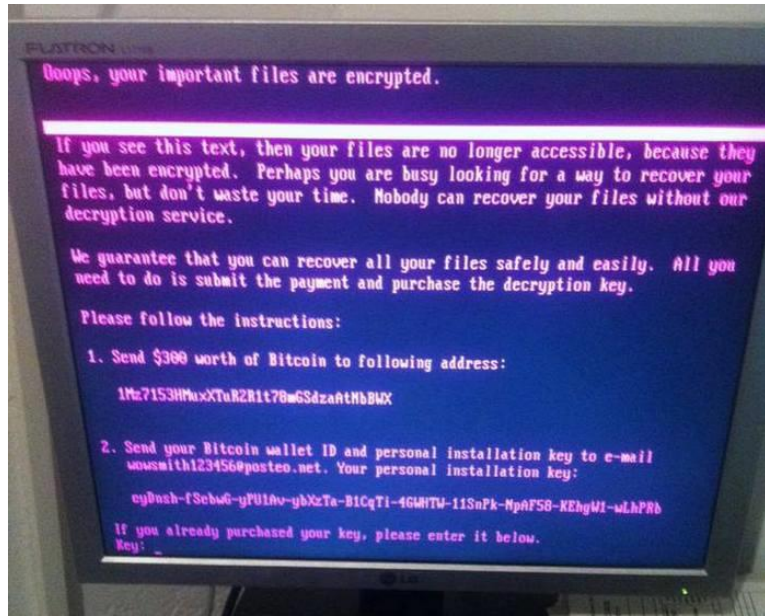
Get WIRED
Access

SUBSCRIBE

UNIVERSITY OF TWENTE.



PETYA RANSOMWARE



800,000 SonicWall VPNs vulnerable to new remote code execution bug

VPN vulnerabilities — the gift that keeps on giving (to attackers).



By Catalin Cimpanu for Zero Day | October 16, 2020 -- 05:00 GMT (06:00 BST) | Topic: Security



Image: SonicWall

Almost 800,000 internet-accessible SonicWall VPN appliances will need to be updated and patched for a major new vulnerability that was disclosed on Wednesday.

Discovered by the Tripwire VERT security team, CVE-2020-5135 impacts SonicOS, the operating system running on SonicWall Network Security Appliance (NSA) devices.

SonicWall NSAs are used as firewalls and SSL VPN portals to filter, control, and allow employees to access internal and private networks.

Tripwire researchers say SonicOS contains a bug in a component that handles custom protocols.

ZDNET RECOMMENDS



Best security cameras for business in 2020: Google Nest, Ring, Arlo, and more

When deciding on a work

MORE FROM CATALIN CIMPANU



Google
How to enable Chrome's secret new Read Later feature



Security
Hacker steals \$24 million from cryptocurrency service 'Harvest Finance'



Security
Adware found in 21 Android apps with more than 7 million downloads



Security
Over 100 irrigation systems left exposed online without a password

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address

SUBSCRIBE

SEE ALL

Millions of Hotel Guests Worldwide Caught Up in Mass Data Leak



Author:
Tara Seals

November 9, 2020
/ 10:43 am

3:30 minute read

[Write a comment](#)

Share this article:



A cloud misconfiguration affecting users of a popular reservation platform threatens travelers with identity theft, scams, credit-card fraud and vacation-stealing.

A widely used hotel reservation platform has exposed 10 million files related to guests at various hotels around the world, thanks to a misconfigured Amazon Web Services S3 bucket. The records include sensitive data, including credit-card details.

Prestige Software's "Cloud Hospitality" is used by hotels to integrate their reservation systems with online booking websites like Expedia and Booking.com.

The incident has affected 24.4 GB worth of data in total, according to the security team at Website Planet, which uncovered the bucket. Many of the records contain data for multiple hotel guests that were grouped together on a single reservation; thus, the number of people exposed is likely well over the 10 million, researchers said.



Ontdek waar
bij u de groei zit



KLIK HIER

Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online

Simon Thomsen, Business Insider Australia

 Jul. 20, 2015, 9:31 AM
  1,977

 FACEBOOK
  LINKEDIN
  TWITTER
  EMAIL
  PRINT

Around 37 million people will be extremely nervous Monday after the extramarital-affair website Ashley Madison was hacked and the details posted online. The Canadian-based site sells itself with the slogan "Life is short. Have an affair."

Data security expert and blogger Brian Krebs revealed [the hack on his site](#), [Krebs On Security](#), saying a group calling itself The Impact Team was behind the hack and said it had stolen user databases, financial records including salary information, and other records.

Krebs says Ashley Madison's parent company, Avid Life Media (ALM), which also runs Cougar Life and Established Men, [acknowledged the breach](#), with CEO Noel Biderman saying the company was "working diligently and feverishly" to delete the release of IP.





The hackers have threatened to release more customer data if Ashley Madison isn't taken down.

Recommended For You



People are using Airbnb for hookups around the world — and the company isn't happy about it



Zakenauto
van het jaar 2016



Vanaf € 142,- netto
bijtelling p.m.*

*op basis van 42% inkomstenbelasting.

[Ontdek meer](#)



Mercedes-Benz
The best or nothing.

Videos You May Like

ANDY GREENBERG SECURITY 11.28.17 05:47 PM

ANYONE CAN HACK MACOS HIGH SIERRA JUST BY TYPING "ROOT"



CHRISTOPH DERNBACH/AP

THERE ARE HACKABLE security flaws in software. And then there are those that don't even require hacking at all—just a knock on the door, and asking to be let in. Apple's macOS High Sierra has the second kind.

On Tuesday, security researchers disclosed a bug that allows anyone a blindingly easy method of breaking that operating system's security protections. When anyone hits a prompt in

UNIVERSITY OF TWENTE.



\$733.70

EUR €694.08

¥5,169.54

GBP £589.54

Earn up to 75%
on each correct choice

Select an asset:

BTC/USD

UP



Will BTC/USD go up or down in next 24 hours?

DOWN



ETHEREUM • NEWS

The DAO Attacked: Code Issue Leads to \$60 Million Ether Theft

Michael del Castillo (@DelRayMan) | Published on June 17, 2016 at 14:00 GMT

NEWS



472

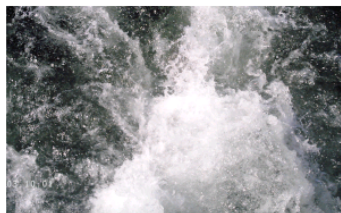


465



The DAO, the distributed autonomous organization that had collected over \$150m worth of the cryptocurrency ether, has reportedly been hacked, sparking a broad market sell-off.

A [leaderless organization](#) comprised of a series of smart contracts written on the ethereum codebase, The DAO has lost [3.6m ether](#), which is currently sitting in a separate wallet after being split off into a separate grouping dubbed a "child DAO".



Ether markets plunged on the news, falling below \$13 in trading on the cryptocurrency exchange Poloniex. With ether currently trading at roughly \$17.50 per coin, that puts the value of the stolen cryptocurrency at more than \$60m.

News of the hack first began to circulate on Reddit and other social media sites this morning, prompting Ethereum co-founder Vitalik Buterin to [call for a pause](#) in trading in ether markets as

DON'T MISS A SINGLE STORY

Subscribe to our free newsletter and follow us

Email Address

SUBSCRIBE

consensus
2017

Registration Is Open!

Only 75 tickets available at \$999

REGISTER NOW

FEATURES



Steemit's First 'Fest'
Reveals the Power of
Blockchain Community



Why Remittance Giant
MoneyGram Won't Be First
With Blockchain



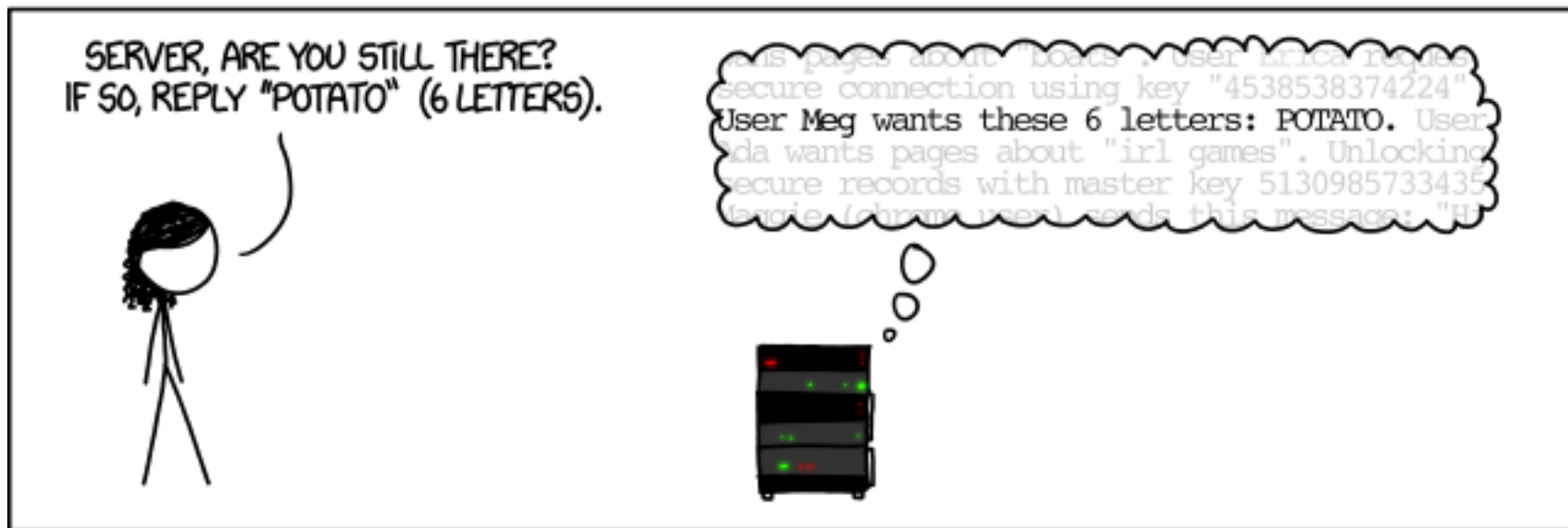
Overstock Could Raise \$30
Million With Blockchain
Stock Offering

Heartbleed

Implementation mistake
in OpenSSL.

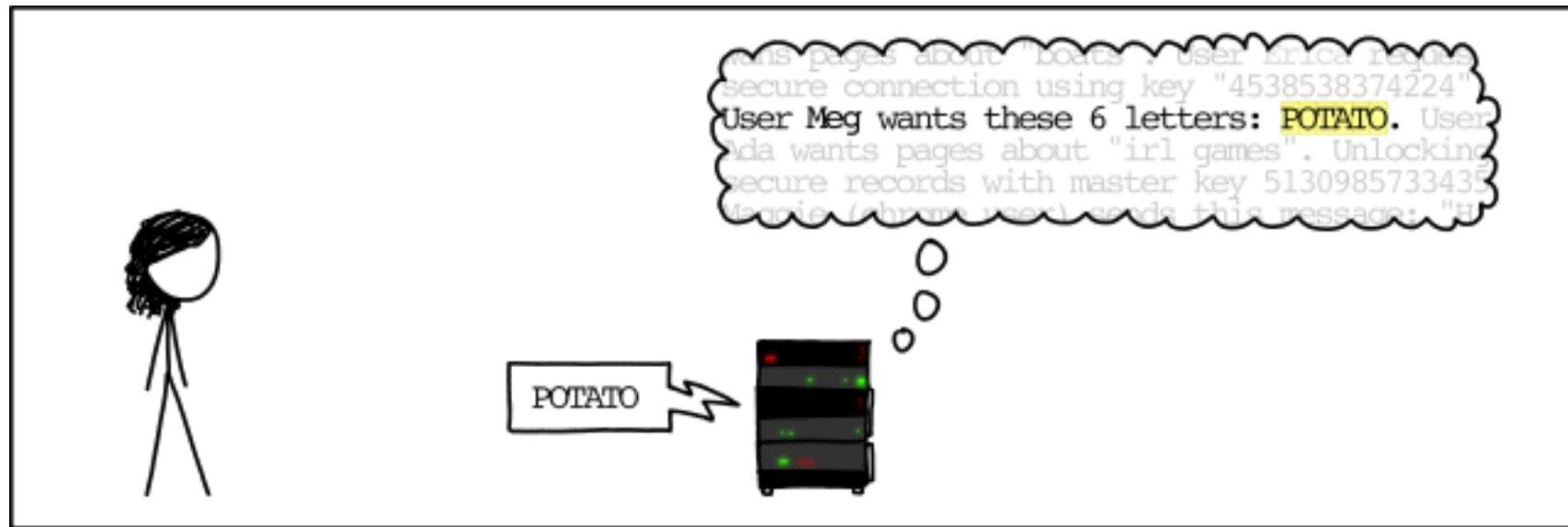


HOW THE HEARTBLEED BUG WORKS:



From: <http://xkcd.com/1354/>

HOW THE HEARTBLEED BUG WORKS:



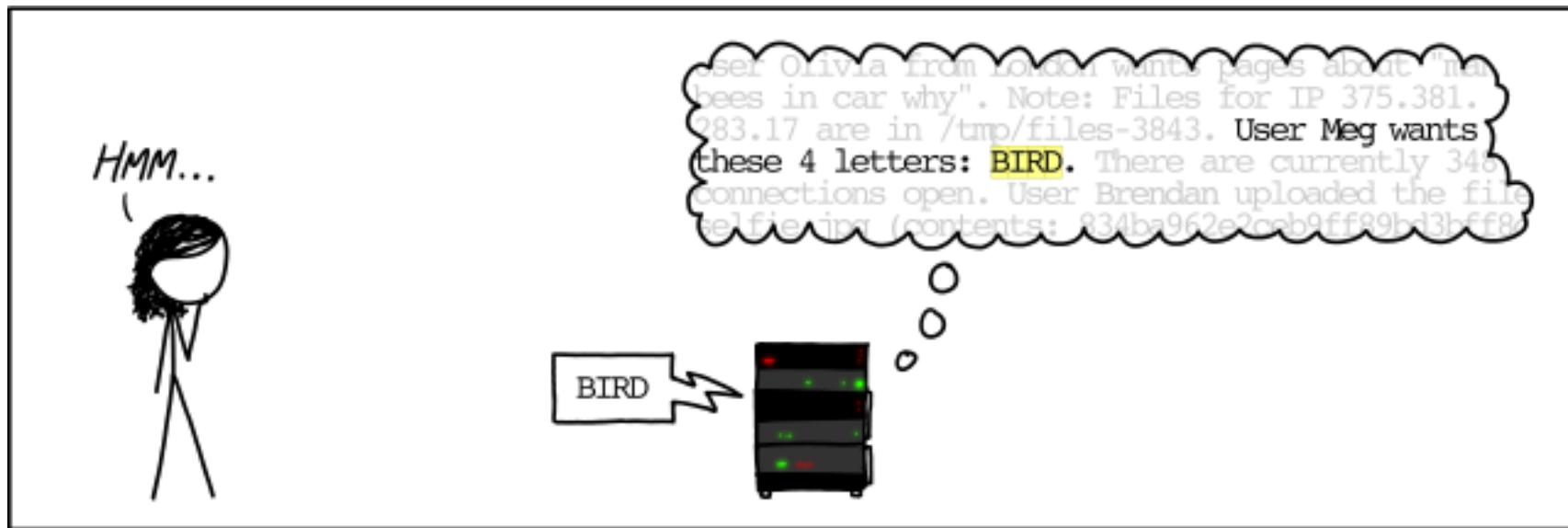
From: <http://xkcd.com/1354/>

HOW THE HEARTBLEED BUG WORKS:



From: <http://xkcd.com/1354/>

HOW THE HEARTBLEED BUG WORKS:



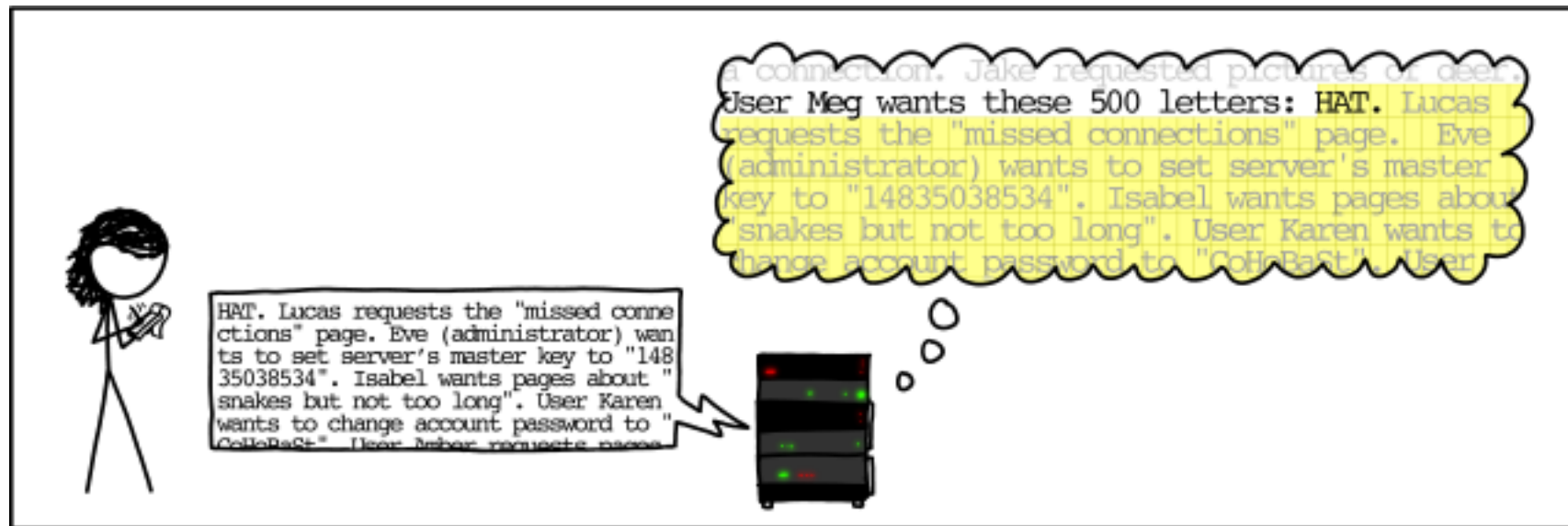
From: <http://xkcd.com/1354/>

HOW THE HEARTBLEED BUG WORKS:



From: <http://xkcd.com/1354/>

HOW THE HEARTBLEED BUG WORKS:



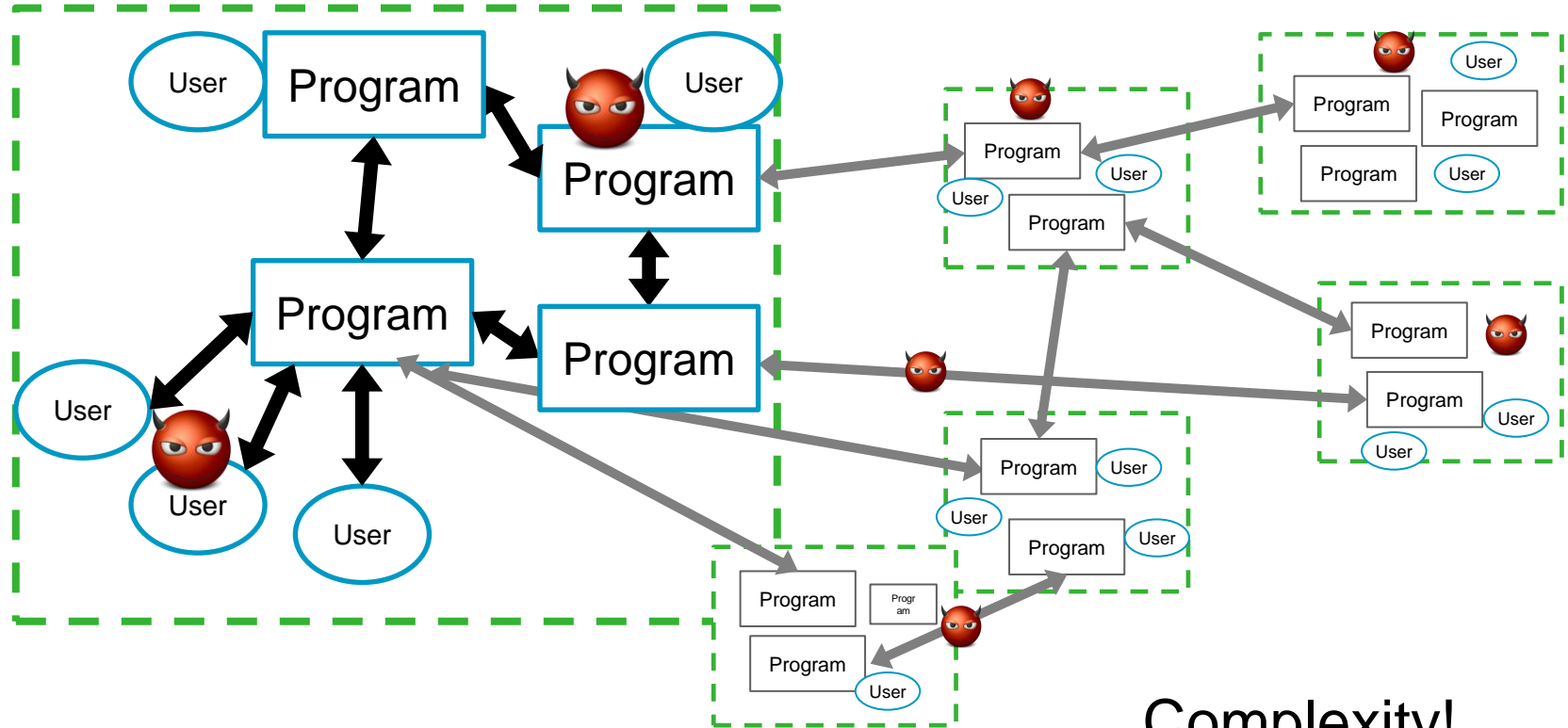
From: <http://xkcd.com/1354/>

Stagefright

- Group of software bugs in Android's "Stagefright" component (a library for media handling)
- Allows for remote code execution and privilege escalation.
- Millions of vulnerable phones.



WHY ARE THERE SECURITY PROBLEMS?



KISS

principle

KEEP
IT
SIMPLE,
STUPID

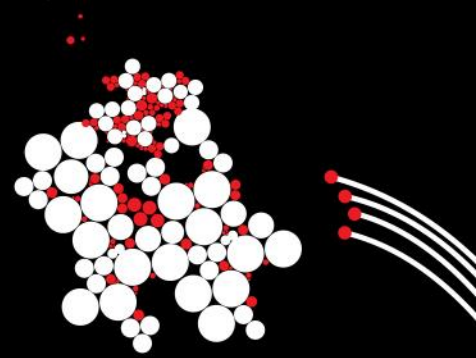
WHY IS SECURITY SO HARD?

1. The defender must defend all points; the attacker can choose the weakest point.
2. The defender can defend only against known attacks; the attacker can probe for unknown vulnerabilities.
3. The defender must be constantly vigilant; the attacker can strike at will.
4. The defender must play by the rules; the attacker can play dirty.

“A good attack is one that the engineers never thought of.”

—Bruce Schneier

From: Writing Secure Code - Howard and LeBlanc



Why security (engineering)?

Topic of Software Systems (TCS module 2)

Lecturer: Maarten Everts

