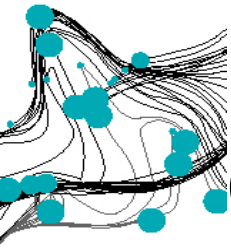
UNIVERSITY OF TWENTE.

PROGRAMMING

3.3 SECURITY ENGINEERING (1)

MODULE 1.2: SOFTWARE SYSTEMS

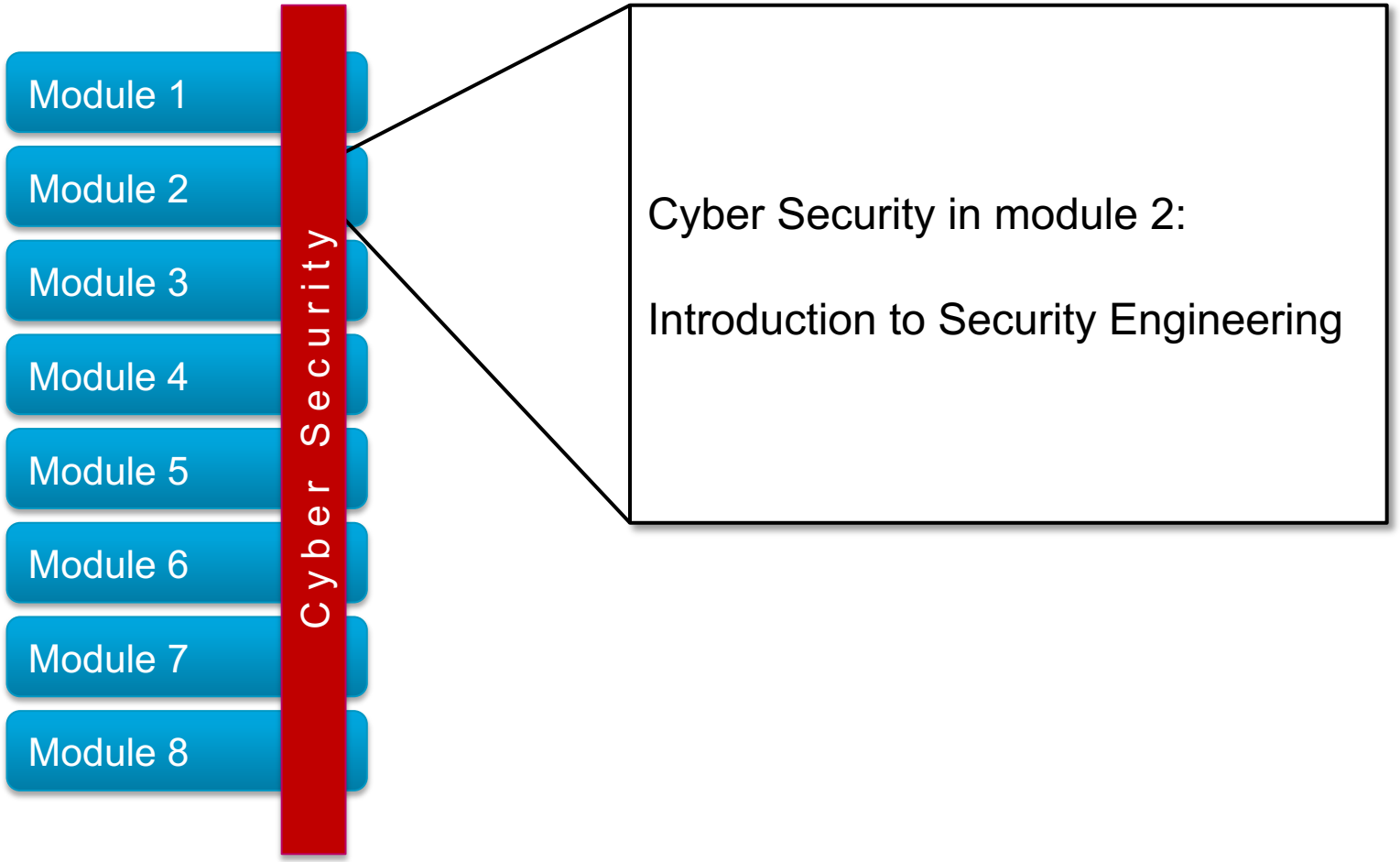
NOVEMBER 29, 2019 – MAARTEN EVERTS



OVERVIEW PROGRAMMING LINE

Week 1 Values and variables Classes and objects	**Week 2** Classes and objects Testing	**Week 3** Interfaces and Inheritance Subtyping Security 1
Week 4 Arrays and lists List implementations Collections	**Week 5** Stream I/O and MVC Exceptions Security 2	**Week 6** Concurrency Project kick-off IDE Tips & Tricks
Week 7 Basic Networking Networking and multithreading GUIs	**Week 8/9** Advanced Java facilities Test	**Week 10** Project Test resit

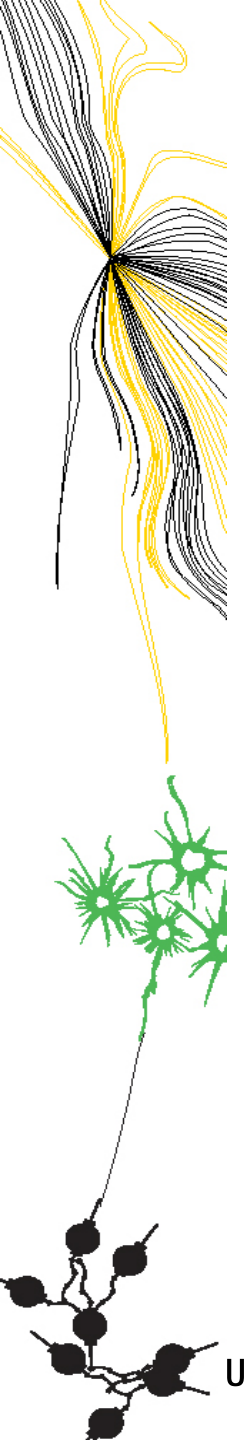
CROSS-CUTTING CONCERN *CYBER SECURITY*



WHAT IS SECURITY ENGINEERING?

"Security engineering is about building systems to remain dependable in the face of malice, error, or mischance." – R.J. Anderson

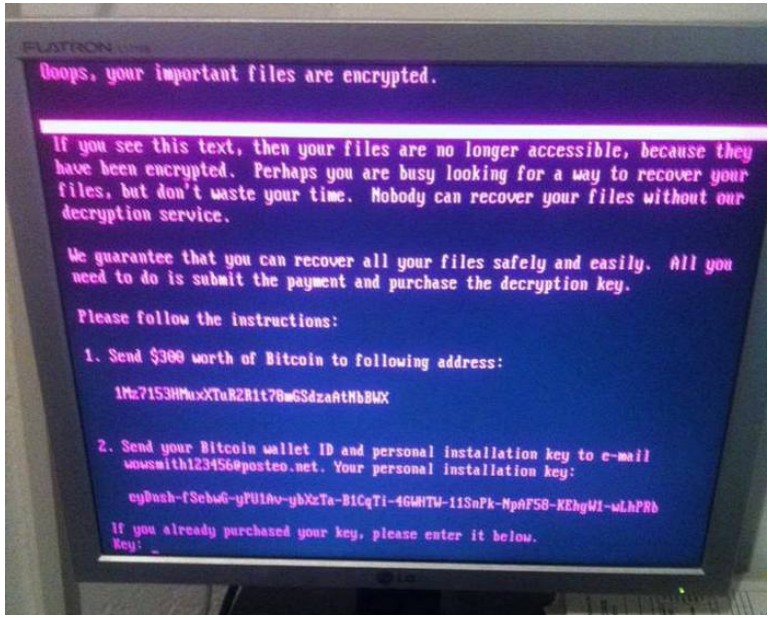
Security engineering is a specialized field of engineering that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts. Wikipedia



SECURITY ISSUES IN THE NEWS


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

PETYA RANSOMWARE



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS SIGN

BIZ & IT —

Why the Equifax breach is very possibly the worst leak of personal info ever

Consumers' most sensitive data is now in the open and will remain so for years to come.

DAN GOODIN - 9/8/2017, 8:09 AM

US Navy

259

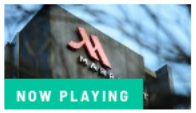
It's a sad reality in 2017 that a data breach affecting 143 million people is dwarfed by other recent hacks—for instance, the ones hitting Yahoo in 2013 and 2014, which exposed personal details for 1 billion and 500 million users respectively; another that revealed account details for 412 million accounts on sex and swinger community site AdultFriendFinder last year; and an eBay hack in 2014 that spilled sensitive data for 145 million users.

The breach Equifax reported Thursday, however,

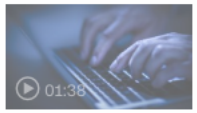
guests

By Jordan Valinsky, CNN Business

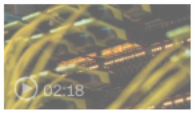
Updated 1824 GMT (0224 HKT) November 30, 2018



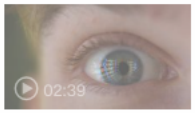
Marriott's guest reservation system hacked



These are some of the most notorious data breaches



How to protect yourself from hackers



Here's why it's so hard to spot deepfakes

New York (CNN Business) – Marriott says its guest reservation system has been hacked, potentially exposing the personal information of approximately 500 million guests.

The hotel chain said Friday the hack affects its Starwood reservation database, a group of hotels it bought in 2016 that includes the St. Regis, Westin, Sheraton and W Hotels.

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

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."

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

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.

Recommended For You


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

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

Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm

REUTERS

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

September 20, 2013 – 10:02 AM

Documents from the archive of whistleblower Edward Snowden indicate that Britain's GCHQ intelligence service was behind a cyber attack against Belgacom, a partly state-owned Belgian telecoms company. A "top secret" Government Communications Headquarters (GCHQ)

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

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,

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

Hackers Are Holding Baltimore Hostage: How They Struck and What's Next

systems that run Baltimore's government.

It could take months of work to get the disrupted technology back online. That, or the city could give in to the hackers' ransom

Latest on Cyber Security

Cyber attacks are a new front in assessing corporate risk

Data hacks and big fines drive cyber insurance growth

Are user data protection rules fit for purpose?

Retailers brace for cyber attacks in peak shopping season

Cyber Security + Add to myFT

WhatsApp voice calls used to inject Israeli spyware on phones

Messaging app discovers vulnerability that has been open for weeks

Save

WhatsApp said teams of engineers had worked around the clock to close the vulnerability © FT montage/Dreamstime

Mehul Srivastava in Tel Aviv MAY 14 2019

337

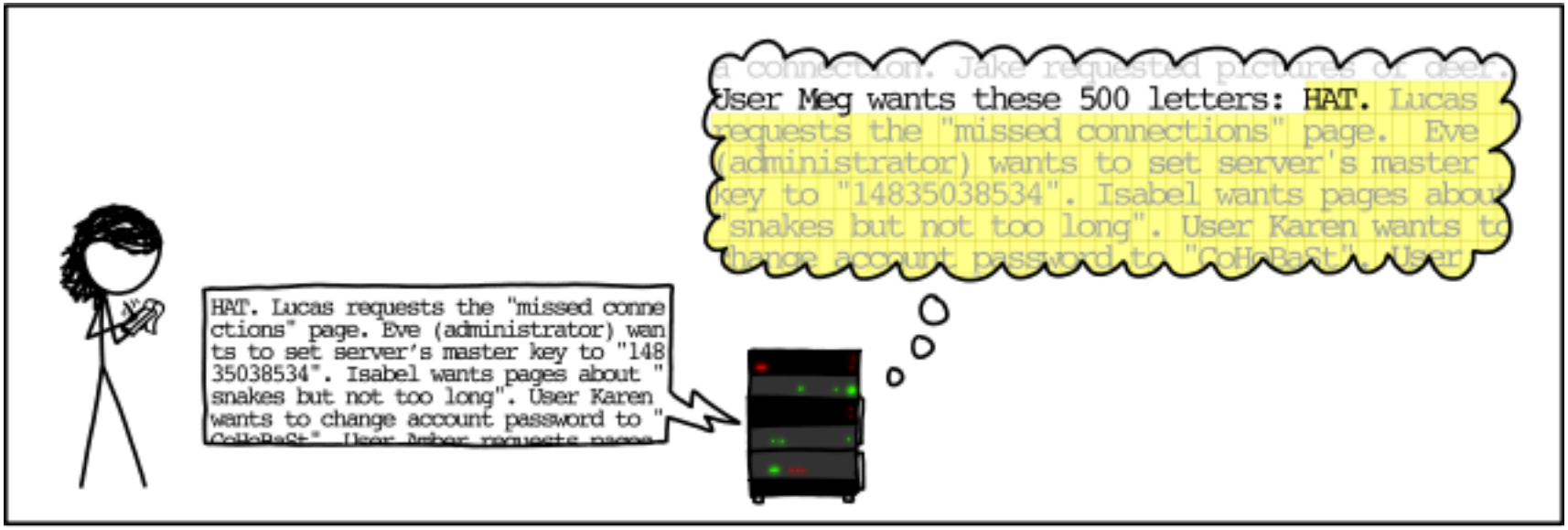
A vulnerability in the messaging app WhatsApp has allowed attackers to inject commercial Israeli spyware on to phones, the company and a spyware technology dealer said.

Feedback

Heartbleed

Implementation mistake in OpenSSL.

HOW THE HEARTBLEED BUG WORKS:



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

Stagefright

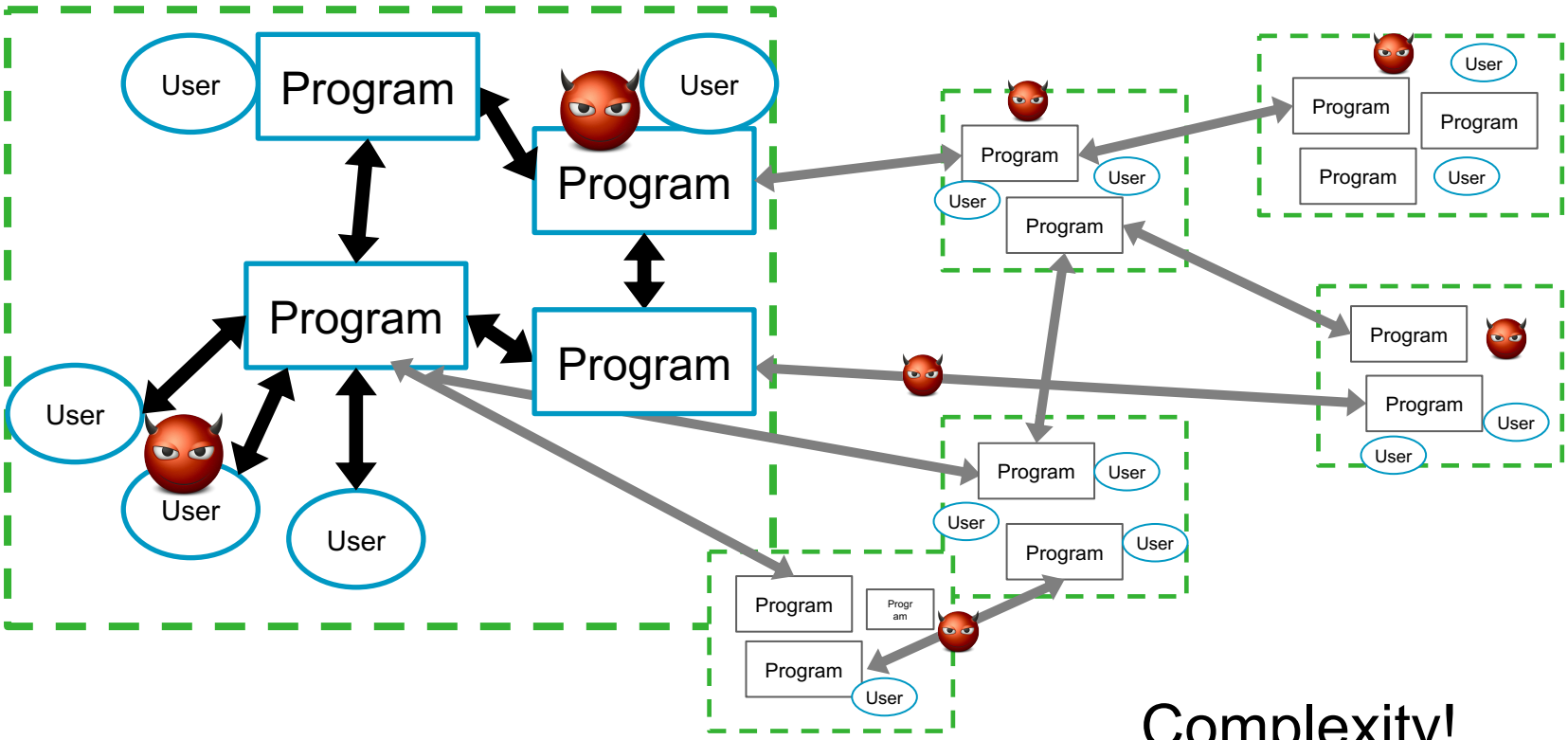
- Group of software bugs in Android's "Stagefright" component (a library for media handling)
- Allows for remote code excution and priviledge escalation.
- Millions of vulnerable phones.

goto fail;

```
38  static OSStatus
39  SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
40                                   uint8_t *signature, UInt16 signatureLen)
41  {
42      OSStatus        err;
43      //...
44
45      if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
46          goto fail;
47      if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
48          goto fail;
49          goto fail;
50      if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
51          goto fail;
52      //...
53
54  fail:
55      SSLFreeBuffer(&signedHashes);
56      SSLFreeBuffer(&hashCtx);
57      return err;
```

- Logic error in Apple's certificate checking code
- Code conventions?
- Could've been found by static analysis

SECURITY? WHY?



KISS

principle

KEEP IT SIMPLE, STUPID

WHY IS SECURITY HARD?

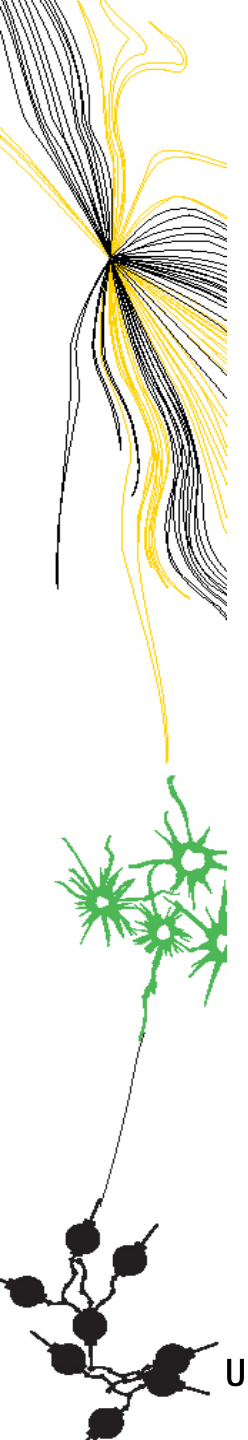
1. The defender must defend all points; the attacker can choose the weakest point.
2. The defender can defend only against known attacks; the attacker can probe for unknown vulnerabilities.
3. The defender must be constantly vigilant; the attacker can strike at will.
4. The defender must play by the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

From: Writing Secure Code - Howard and LeBlanc

"A good attack is one that the engineers never thought of."
–Bruce Schneier

SECURITY SUBJECTS NOT COVERED

- Mathematics behind cryptography [module 1]
- History of cryptography [module 1]
- How to implement cryptographic primitives
- How to deal with user-provided input (e.g., SQL injections) [module 4]
- Reverse Engineering
- Buffer overflows [module 5]
- Exploit development & malware development
- Advanced protocols
- Operating system security & access control [module 5]
- Network security [module 3]
- Securing web-applications [module 4]
- Much more…..



WHAT IS SECURITY?

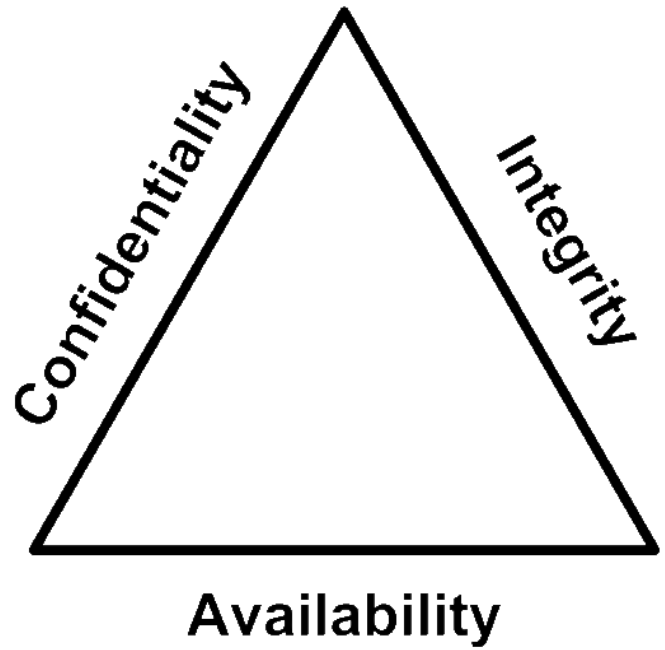
SECURITY PROPERTIES/CONCEPTS/ATTRIBUTES/ASPECTS

Confidentiality

Integrity

Availability

NL, BIV-model:
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid


Confidentiality
Integrity
Availability

CONFIDENTIALITY

Concealment of sensitive information, or:

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes." – [RFC 4949]

Examples:

- Users should not be able to see the bank account balance of other users.
- Someone who finds my phone should not be able to see its content.

Typical security measures:

- Encryption [Module 1]
- Authentication [coming up]
- Access control

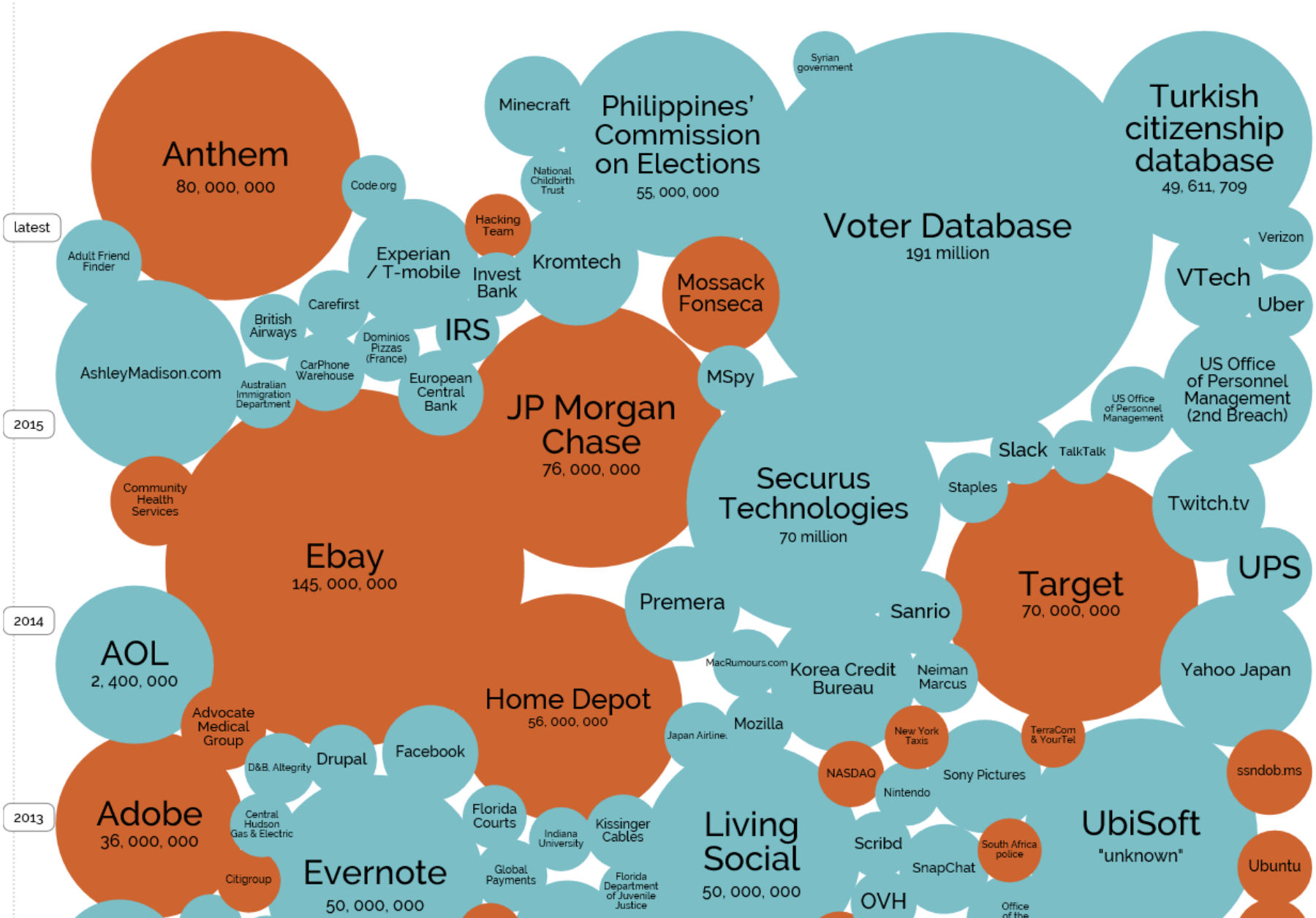
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 6th May 2016)

interesting story

YEAR | BUBBLE COLOUR: YEAR | METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER

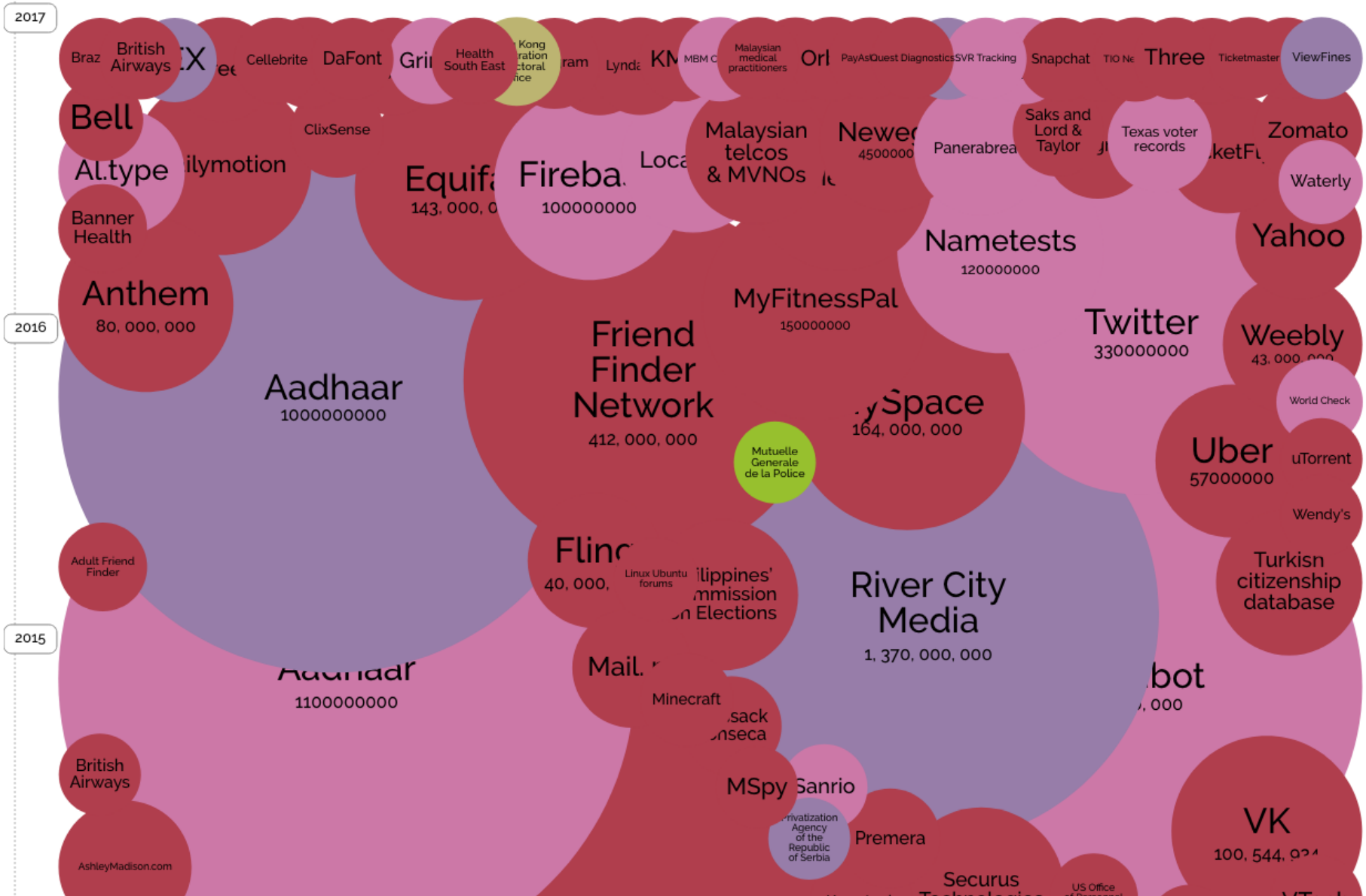


World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 15th Oct 2018)

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

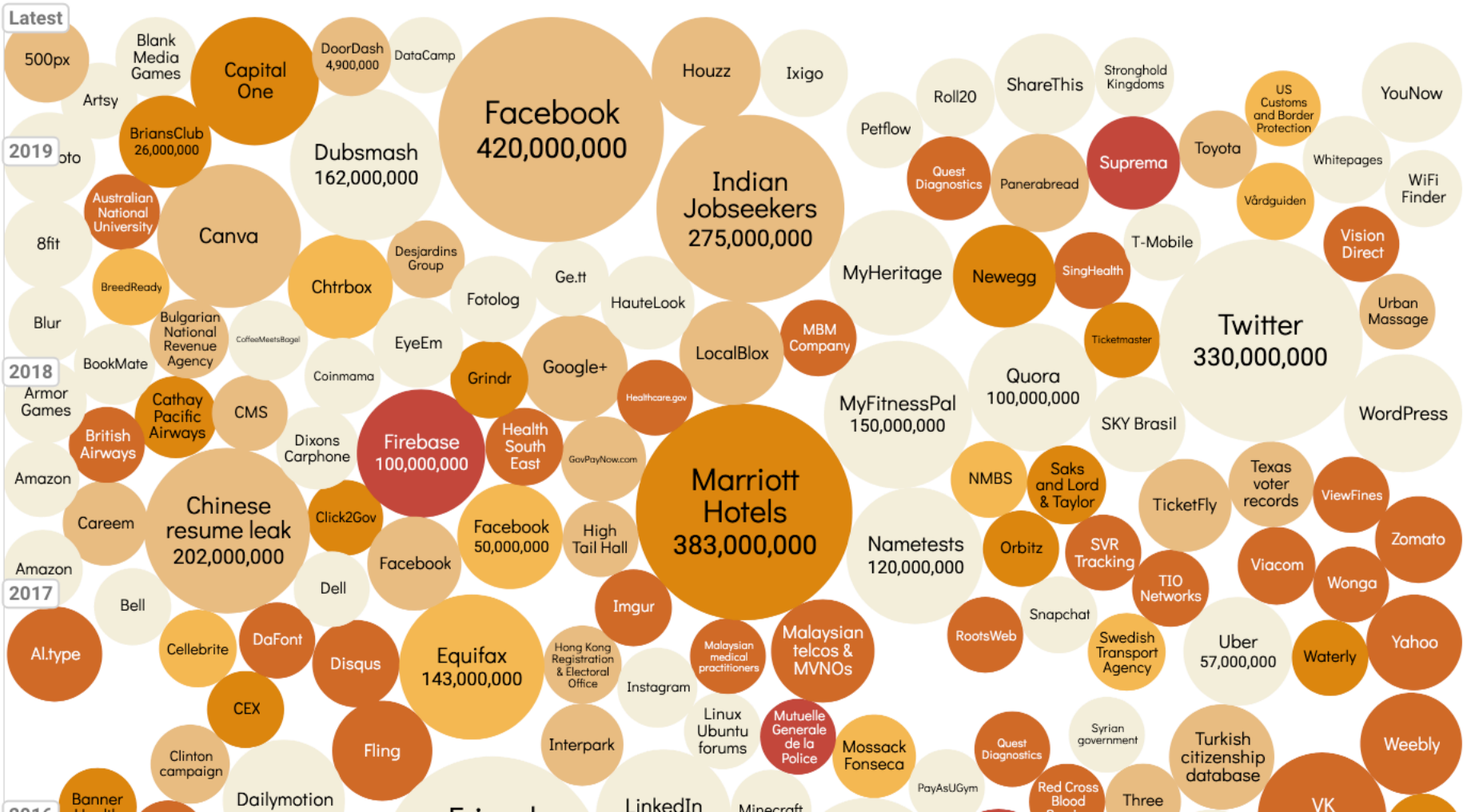
Last updated: 1 April 2019

interesting story

Filter Colour YEAR DATA SENSITIVITY

Low High

Search...

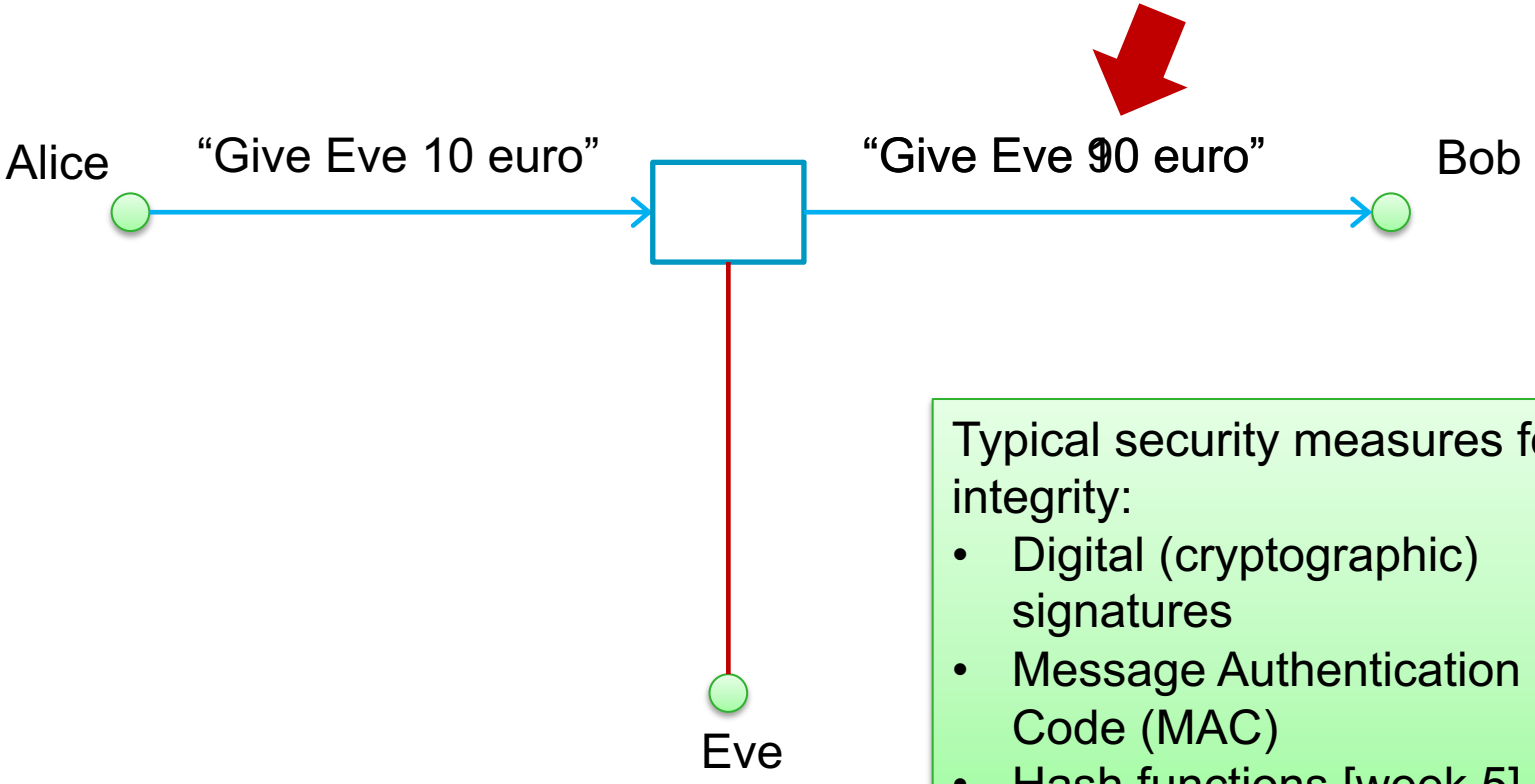


INTEGRITY

Assuring the accuracy and consistency of data, or:
“The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.”

INTEGRITY

INTEGRITY



Typical security measures for integrity:

- Digital (cryptographic) signatures
- Message Authentication Code (MAC)
- Hash functions [week 5]

INTEGRITY

Other examples of integrity failures:

- Manipulation of bank records
- Manipulation of access logs
- Removal of access logs

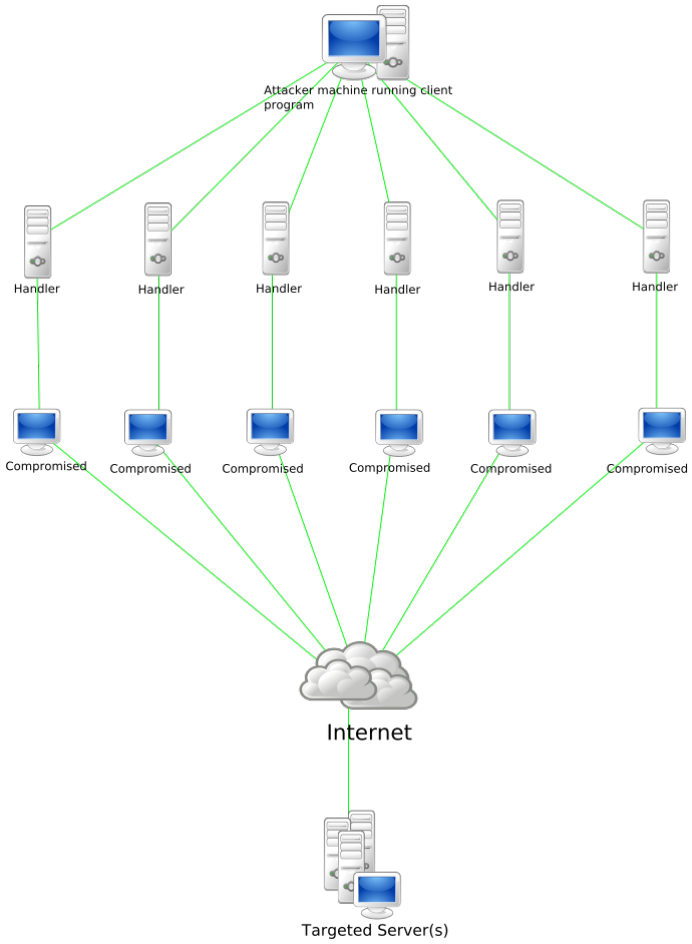
AVAILABILITY

Ability to use the required information or resource.

Availability is the target denial-of-service attacks: they deny the intended users from accessing a resource.

AVAILABILITY

Common example:
Distributed Denial-of-Service (DDoS)



Shopify
Spotify
Twitter
Popular Posts


Airspace can catch high-speed drones all by itself
5 days ago

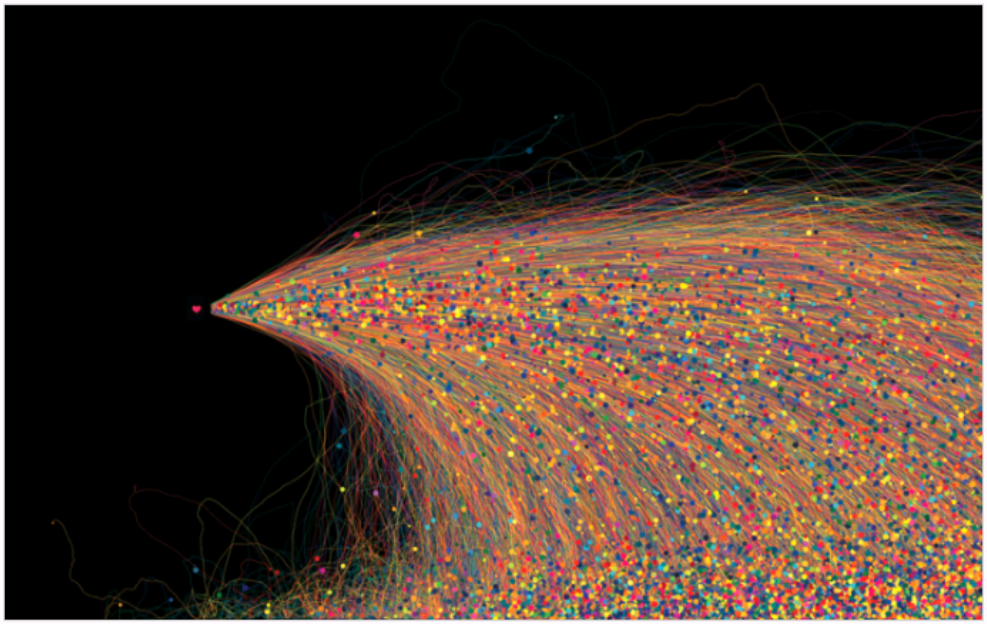

App abandoment is on the rise as consumers stick to the apps they know
5 days ago


This 18-year-old just raised $3.5 million to help developers easily add capabilities to their apps
2 days ago


Google can now tell you how busy a place is before you arrive
3 days ago

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Posted Oct 21, 2016 by Darrell Etherington (@etherington), Kate Conger (@kateconger)



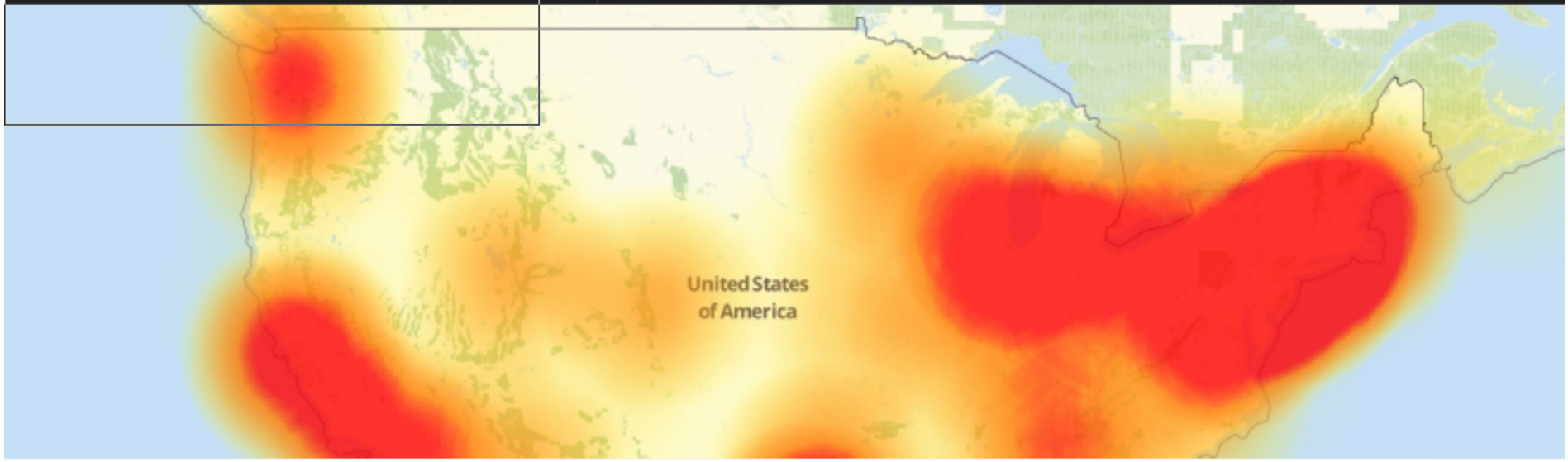
Several waves of major cyberattacks against an internet directory service knocked dozens of popular websites offline today, with outages continuing into the afternoon.

Crunchbase

Shopify –

FOUNDED
2004

OVERVIEW
Shopify is the leading cloud-based, multichannel commerce platform designed for small and medium-



Blame the Internet of Things for Destroying the Internet Today

October 21, 2016 // 04:35 PM EST

Written by
LORENZO FRANCESCHI-BICCHIERAI
STAFF WRITER

A massive botnet of hacked Internet of Things devices has been implicated in the cyberattack that caused a significant internet outage on Friday.

The botnet, which is powered by the malware known as Mirai, is in part responsible for the attack that intermittently knocked some popular websites offline, according to Level 3 Communications, one of the world's largest internet backbone providers, and security firm Flashpoint.

"We are seeing attacks coming from a number of different locations. We're seeing attacks coming from an Internet of Things botnet that we identified called Mirai, also involved in this attack," Dale Drew, chief security officer at Level 3 Communications

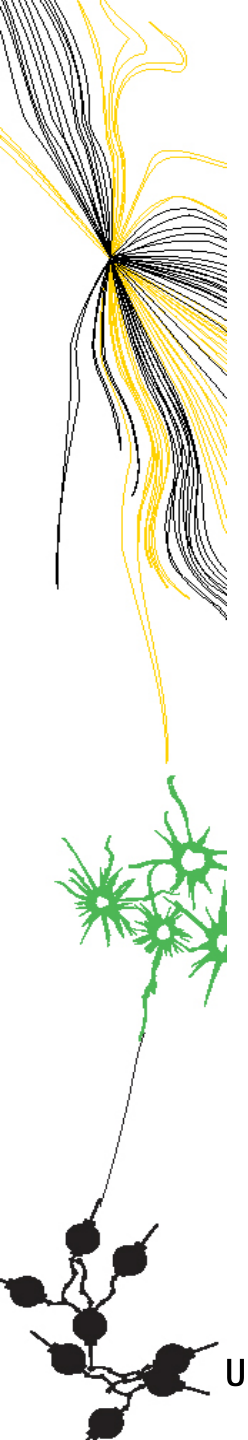
AVAILABILITY

Consider the following code:

```
public static int badIntLog2(int input) {
    int a = input;
    int i = 0;
    while (a != 1) {
        a = a / 2;
        i = i + 1;
    }
    return i;
}
```

What is the output when input = 8? Or 128?

What happens if someone is able to make input -8?

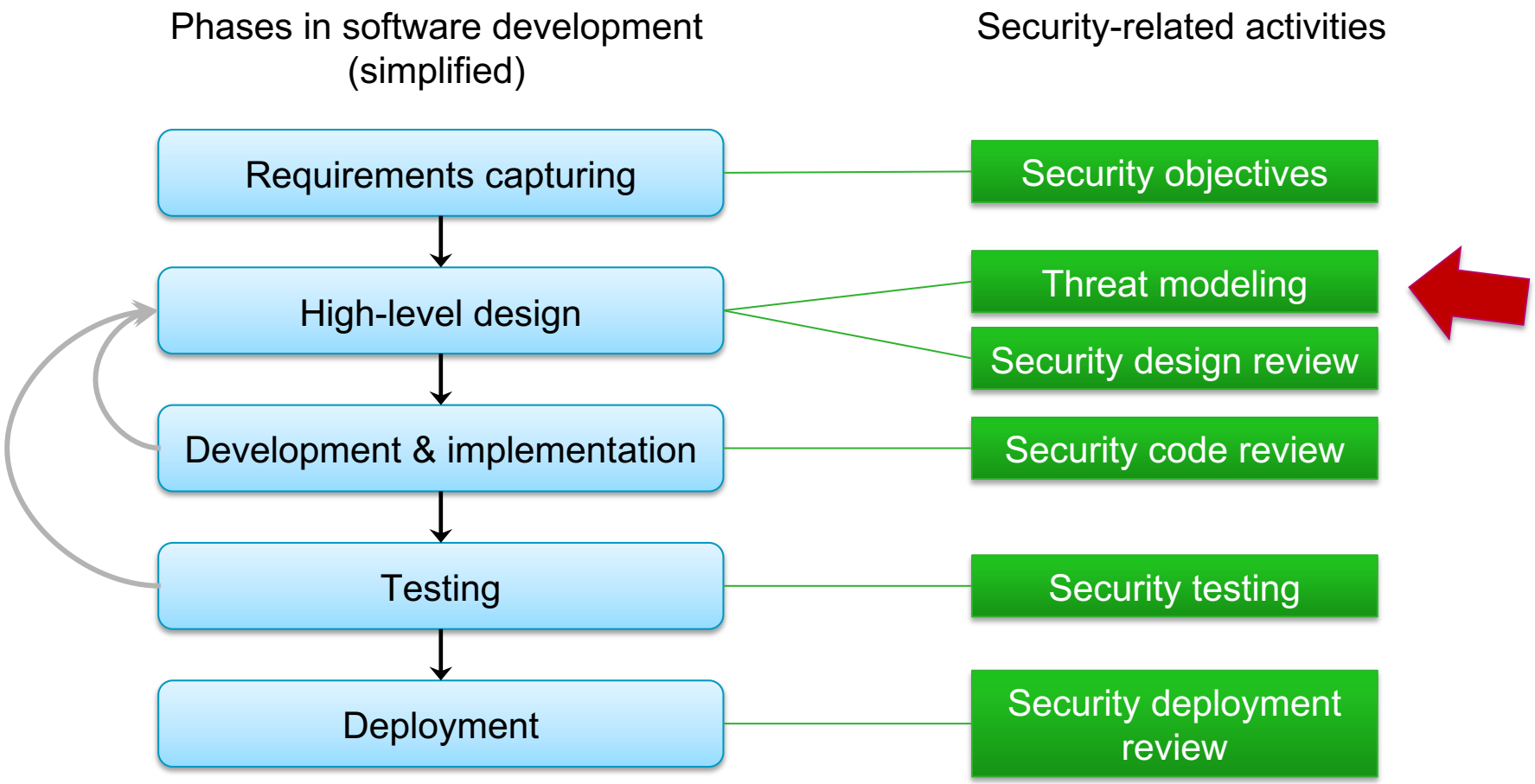


SOFTWARE & SECURITY

TERMINOLOGY IN (SOFTWARE) SECURITY

- Threat: potential violation of security
- Vulnerability: “Security-relevant software defect that can be exploited to effect an undesired behavior”
  - Flaw: defect in design
  - Bug: defect in the implementation
- Exploit

SECURITY IN THE DEVELOPMENT PROCESS

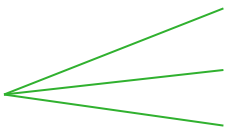


THREAT MODELING (SIMPLIFIED)

Semi-structured approach to identify, quantify and address security risks in an application.

High-level steps:

1. Understanding the application (the design)
2. Identifying & categorizing threats
3. Countermeasures & mitigation

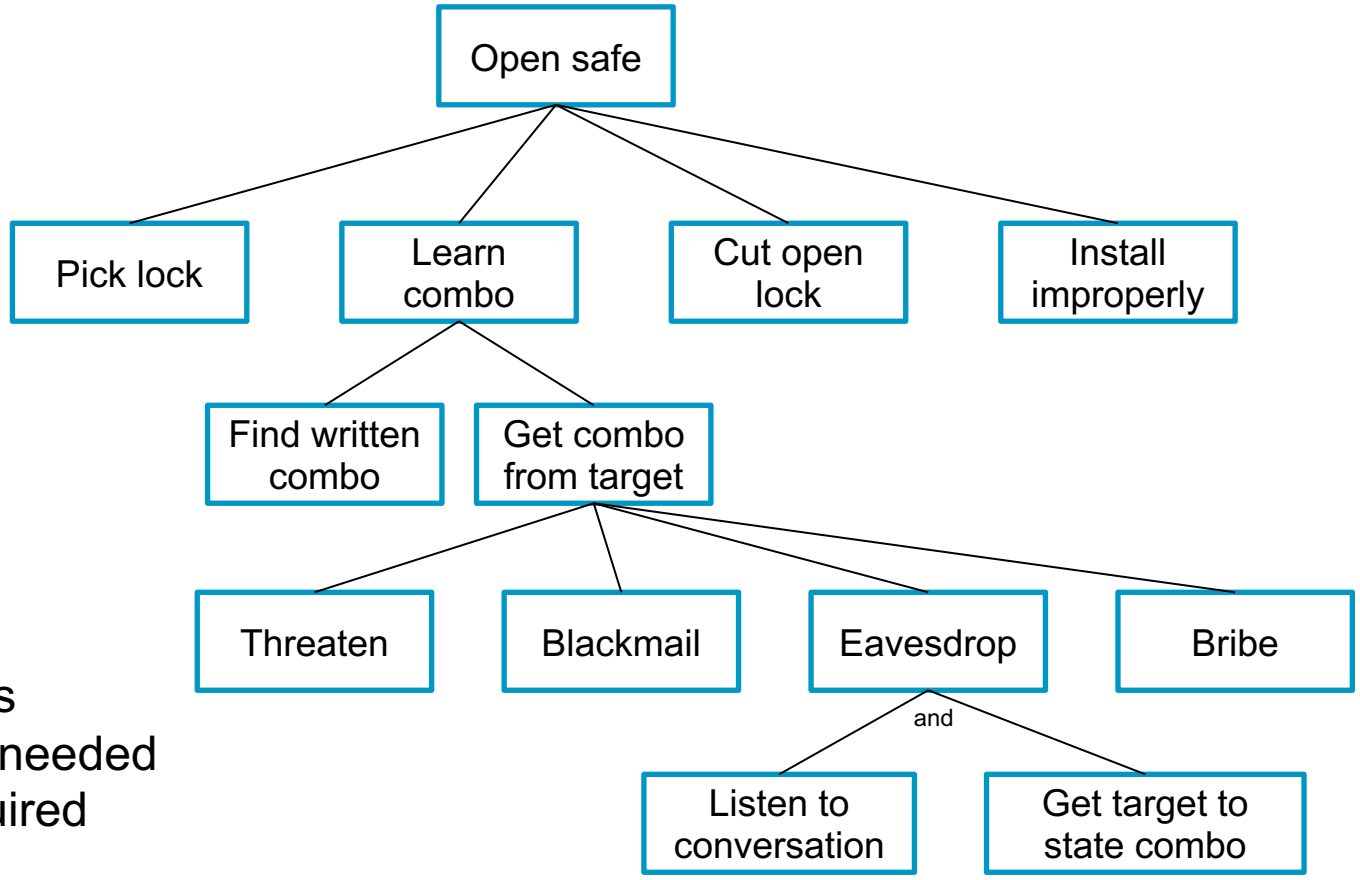


- Identify entry/exit points
- Identify assets
- Identify trust levels

CATEGORIZING THREATS (STRIDE)

- Spoofing: posing as something or somebody else (e.g., replay attacks, phishing attacks)
- Tampering: malicious modification of data or code
- Repudiation: participating in a transaction or communication, and later claiming that the transaction or communication never took place.
- Information Disclosure: exposure or leakage of information
- Denial of Service: render a service or resource useless
- Elevation of Privilege: gaining increased capability

THREAT/ATTACK TREES



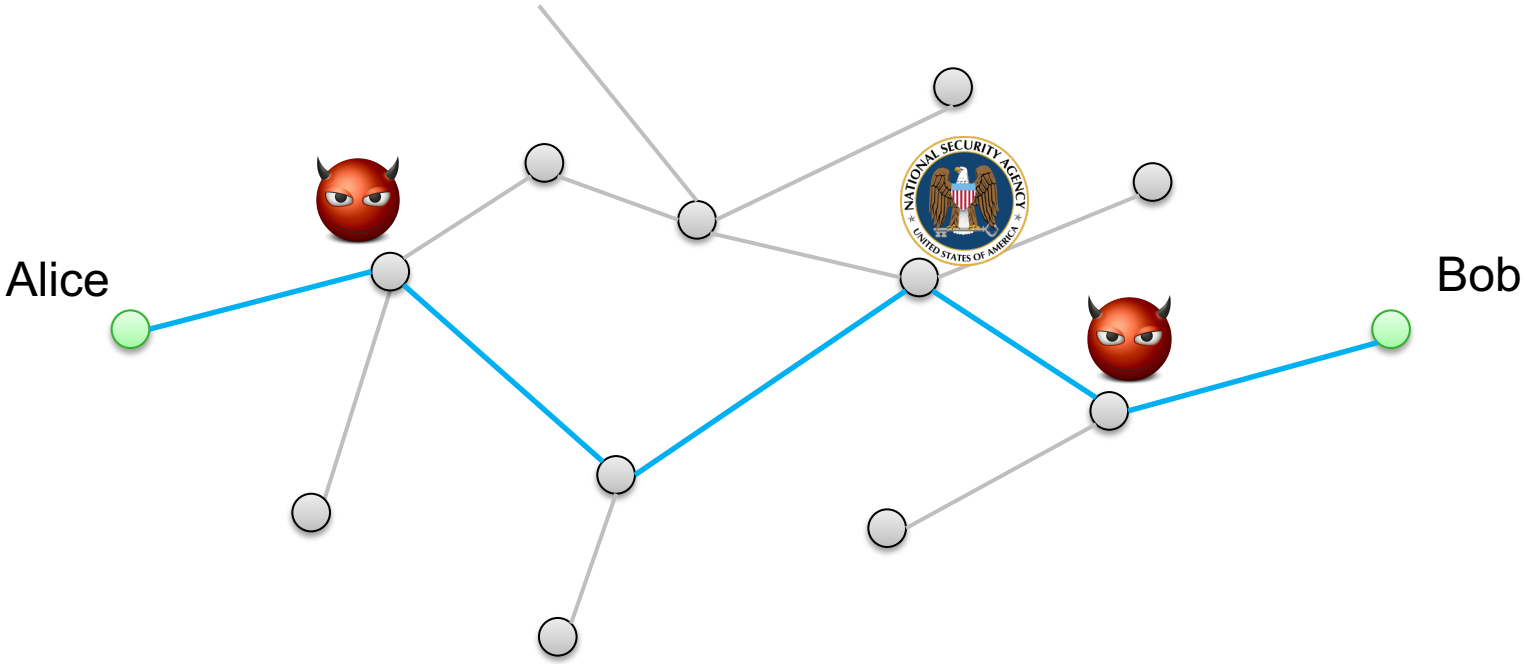
From: https://www.schneier.com/attacktrees.pdf

Extend with:

- Probabilities
- Equipment needed
- Money required

ATTACKER MODELS – FEATURING: ALICE & BOB

ATTACKER MODELS – FEATURING: ALICE & BOB



Passive attacker: only listens

Active attacker: listens & modifies!

Aka, man-in-the-middle

MITIGATION

- Implementation of security features:
  - Cryptography
  - Authorization (access control)
  - Authentication

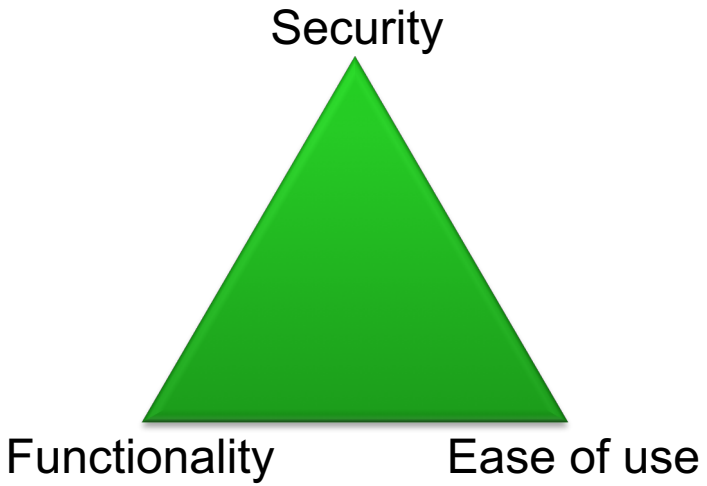
  } No magic bullet! Easy to make mistakes!
- Prevention (of bugs)
  - Testing!
  - Formal specifications (e.g., JML, langsec)
  - Defensive programming
- Detection
- Audits
- Recovery & response

SOME SECURITY DESIGN PRINCIPLES

- Favor simplicity
  - Use fail-safe defaults
  - Do not expect expert users
- Trust with reluctance
  - Employ a small trusted computing base
  - Grant the least privilege possible
    - Promote privacy
    - Compartmentalize
- Defend in Depth
- Monitor and trace

BALANCING SECURITY

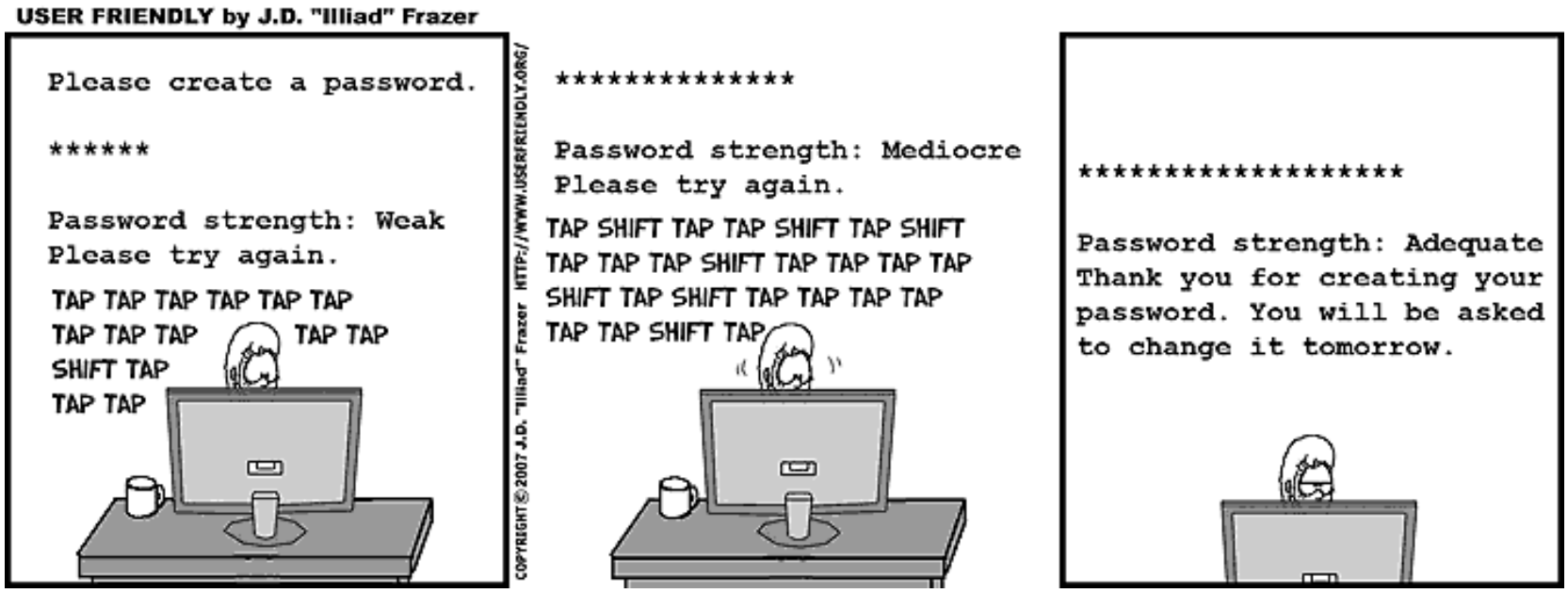
Security vs.
- cost
- performance
- usability
- acceptance

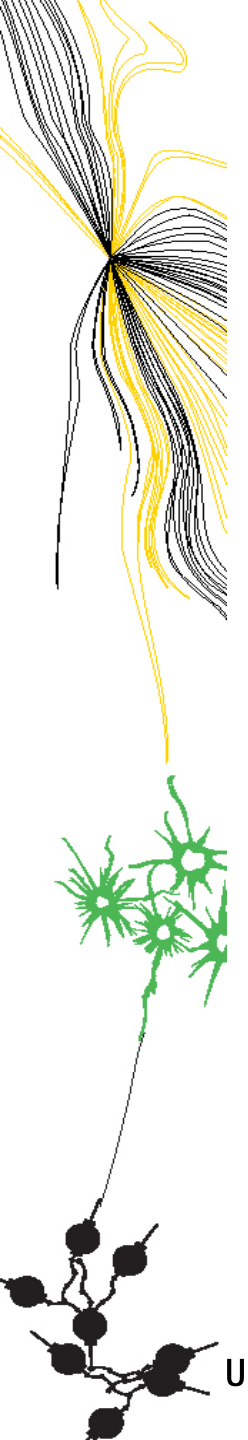


From: http://blog.infosanity.co.uk/2010/06/12/infosec-triads-securityfunctionalityease-of-use/

BALANCING SECURITY

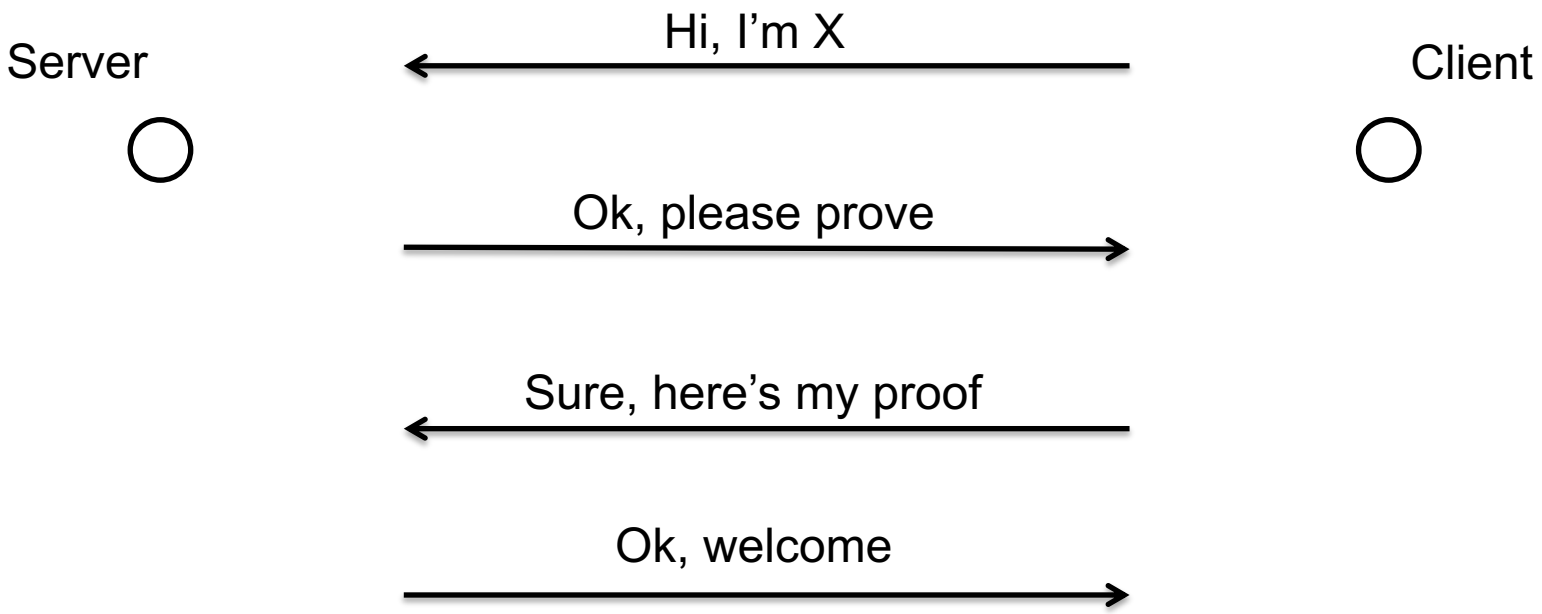
BALANCING SECURITY





AUTHENTICATION

AUTHENTICATION (INFORMAL)



PROVING YOU'RE YOU: FACTORS

Something the user *knows*

Something the user *has*

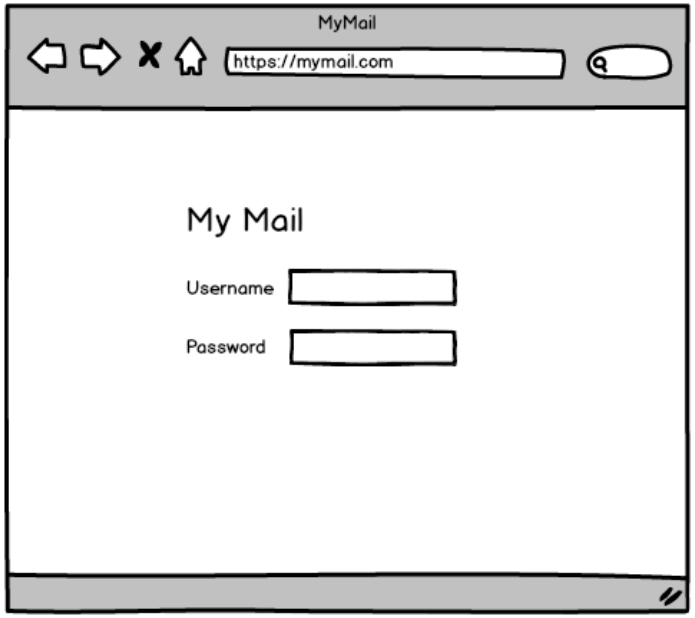
Something the user *is*

Combine for stronger authentication: Multi-factor authentication

SOMETHING THE USER *KNOWS*

Pincodes, passwords & passphrases

PASSWORDS: THE GOOD



Simple & understandable

Familiar & widespread

Portable

Cheap to implement

PASSWORDS: THE BAD

Re-use across domains

Managing

Too simple passwords

Phishing & sniffing

SOMETHING THE USER *HAS*

Essence:

Having *access* to a secret

Many variants:

- Type of secret
  - Shared symmetric key
  - Private key of a asymmetric key pair
- Additional protection
  - Separate device
  - Tamper-proof hardware (token)
  - Pin/password protected

Challenge-response vs. synchronous

RSA SecurID token

- Hardware token
- Tamper-proof
- Synchronous
- Shared symmetric key (seed)
- Sometimes called:
  One Time Password (OTP)

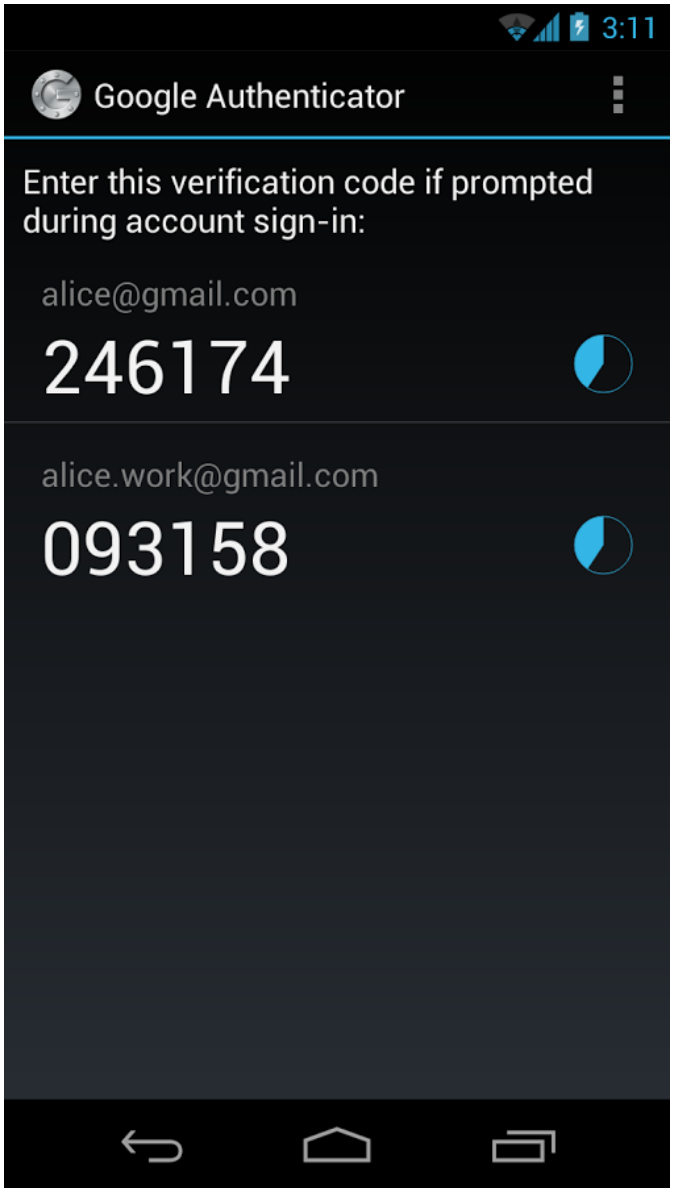
yubico's YubiKey

- Hardware token
- Tamper-proof
- Synchronous
- Shared symmetric key

http://www.yubico.com/

A bank's access token

- Hardware token
- Tamper-proof
- Challenge-response
- Shared symmetric key
- Pin-protected



Google Authenticator

- Separate device (mobile)
- Synchronous
- Shared symmetric key

SOMETHING THE USER *IS*

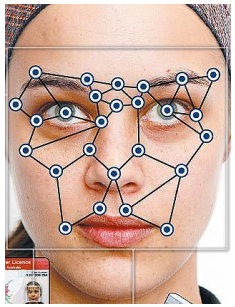
Main idea: using unique personal attributes for authentication

Downsides:

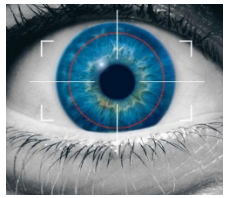
- Intrusive
- Hard to replace
- False positives & negatives
- Complex & expensive

fingerprint

hand geometry



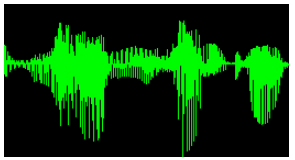
facial scan



iris scan

retina scan

palm scan



voice print

signature dynamics

keyboard dynamics

WHAT WERE THE THREE SECURITY PROPERTIES AGAIN?

Confidentiality

Integrity

Availability

LAB EXERCISES RELATED TO SECURITY

- P-5.7-9 (Hex & Base64 encoding)
- P-6.4-10 (Password cracking & how to properly store them)
- P-7.6 (Networked attack)
- P-7.17 (Bonus: crypto attack)

SECURITY LECTURE IN WEEK 5

- More technical, topics include:
  - Java's security advantages
  - Hash functions
  - Side-channel attacks
  - How to use security-related functionality