Futurae Technologies AG

Grow Wädenswil

29 August 2017

IT Security in Practice

Tailored Overview for Founders and Startup Employees

Claudio Marforio claudio@futurae.com

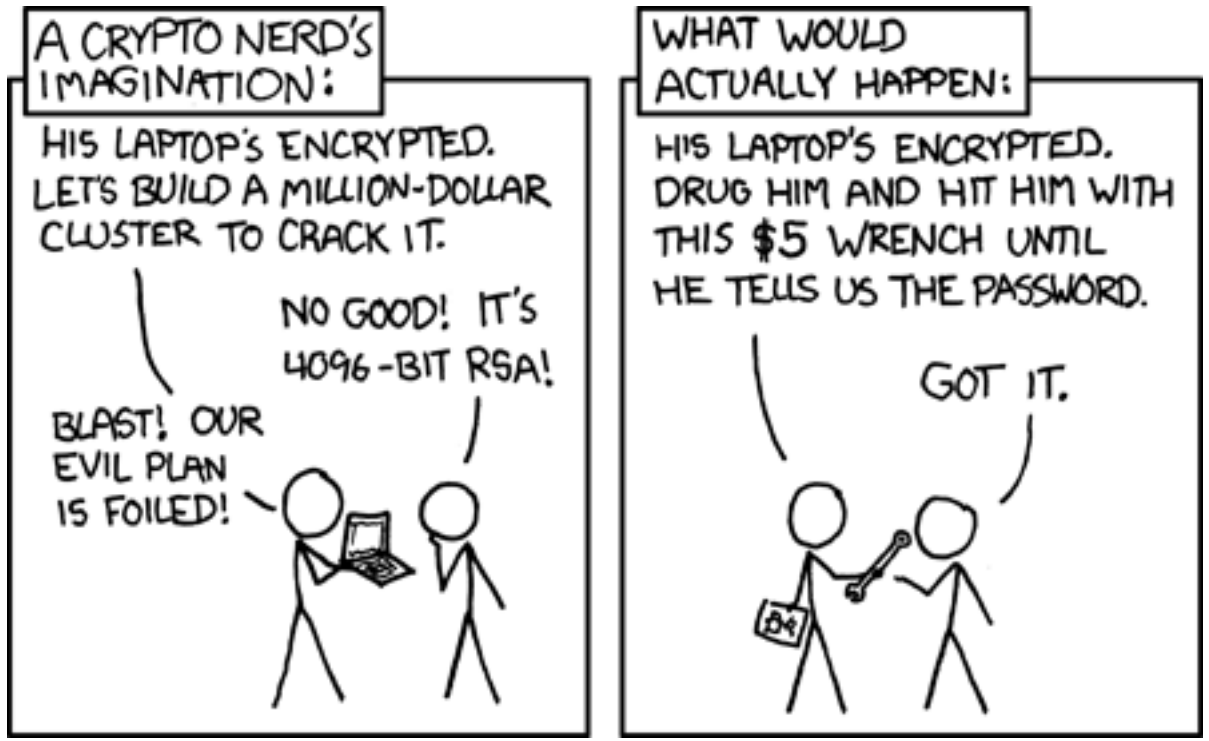
Agenda

- Introduction
- Security Applied:
  - Cryptography / Protocols
  - Communication Tools
  - Mobile Security
  - Data Storage
  - Authentication and Malware
- IT Security Best Practices - Recap
- Discussion

About Me

- Passion for computers since 7
- Bachelor in Computer Science (USI Lugano)
- Master in Computer Science with a focus on Security (ETH Zurich)
- PHD from the System Security Group (ETH Zurich)
  - main research focus: mobile security
- Speaker at top-tier international conferences (NDSS, USENIX Security, CHI, ACSAC, CCS)
- Co-founder of Futurae Technologies AG

Cryptography / Protocols


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Cryptography

- **Authenticity** vs **Confidentiality** vs **Integrity**
  - Authenticity: you know that the message comes from who claims to have sent it
  - Confidentiality: no one but the intended recipient can read the message
  - Integrity: the message hasn't been tampered with

- **Cost**: cryptographic operations can be expensive (in terms of computing power)

- Secure data in transit (over a network) vs. at rest (on your server)

Cryptography

Asymmetric (or Public Key) Cryptography

- Each party has 2 keys: a *private* and a *public* key
- **NEVER** send or share your private key
- The public key can be shared with anyone
- Examples: RSA, DSA, Elliptic Curve
- How to use:
  - Encrypt under the recipient public key: only recipient can decrypt message
  - Sign with your private key: everyone can verify that you sent the message
- Operations can be expensive, use envelope encryption
- Key size is one of the most important parameters
  - 2048 RSA keys (safe until 2030)
  - 224 EC keys (safe until 2030)

Cryptography

Symmetric Cryptography

- Each party has 1 key, which should be **kept secret**
- Examples: AES, 3DES
- How to use:
  - Encrypt your message with the key, only who has the key can decrypt it
- Typically operations are very fast also over large amounts of data (hardware accelerated crypto)
- Different modes of operations – different use cases!
  - Examples: CBC, GCM, XTS, …
- Key size is one of the most important parameters
  - 256 AES keys (safe until 2030)

Cryptography

Hashes and Signatures

- A *hash* maps data of an arbitrary size into data of fixed size
  - (in cryptography, you expect non-invertible hash functions)
- Examples: SHA-256
- How to use:
  - Take a message and pass it through a hash function
  - 590f90a540b98f1a99bfe3048b39fcac1bed5acab335bc368354a43f6709b4a8
- The same input will always result in the same output
- Useful to check that a message has not been changed (*integrity*)
- Can be combined with a key to verify *authenticity* and *integrity*
  - Examples: HMAC

Do not invent your own…

consult an expert, if in doubt

Protocols

- Think what property you want to achieve:
  - Confidentiality
  - Integrity
  - Authenticity
- Typically: a mix of all of them
- Use insights from experts:
  - https://stackoverflow.com/questions/tagged/cryptography
- Use standard libraries:
  - https://www.openssl.org
  - http://bouncycastle.org

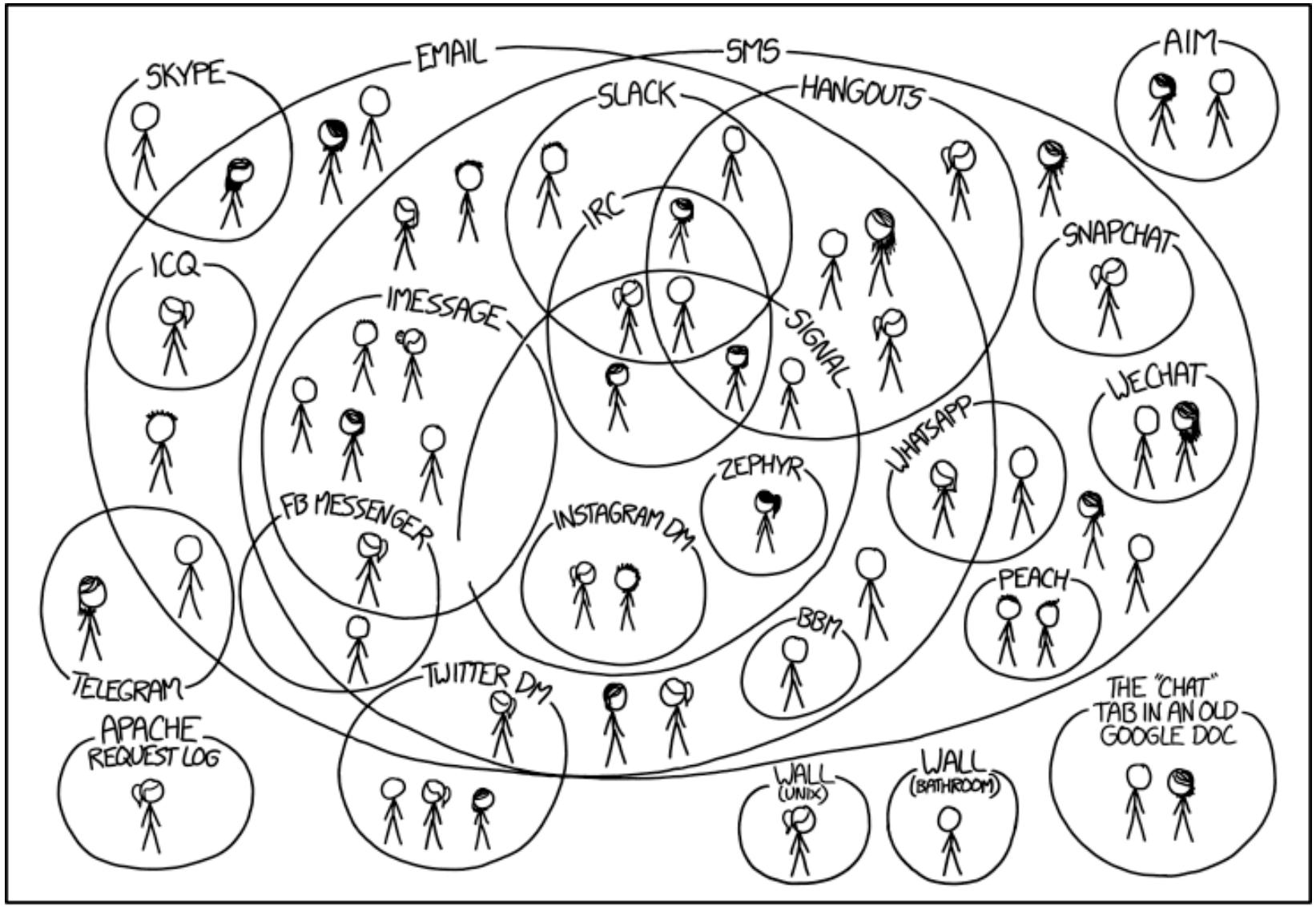
Protocols

- Use HTTPS (TLS) for any network communication
- *Let's encrypt* offers FREE certificates: https://letsencrypt.org
  - it can be a bit tedious to setup, but works well
- Many alternatives exist, go with a known certificate authority
- Examples:
  - Digicert
  - Thawte
  - Globalsign
- *Most probably* you do not need EV (Extended Validation) certificates (the ones used by banks or large enterprises)
- *Most probably* you do not need a *star (*)* certificate

Protocols

- Combining multiple ones can create problems
- Do not re-use cryptographic keys for different protocols
- If security is a top priority for your startup (for your customers, and for marketing) have your protocols checked by an expert
  - Informal analysis (1 day)
  - Formal analysis (1 week)
  - Implementation analysis (2/3 weeks)
- First make something secure, then look for optimizations (that do not break the security)

Communication Tools



I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.

Why care?


PICTURES
PLACES YOU'VE BEEN
(SHARE MY LOCATION)
EMAIL ADDRESSES
PERSONAL PREFERENCES
(LINKS, ARTICLES, MUSIC, ETC)
ONLINE BANKING ACCESS CODES
EX: 287451
DOCUMENTS
INSTANT MESSAGES
& TEXT MESSAGES
POSTAL ADDRESSES
SCAN OF IDS
TWO-FACTOR AUTHENTIFICATION CODES
DETAILS ABOUT RELATIONSHIPS
PHONE NUMBERS

What is NOT secure

- SMS
  - Interceptable
  - Modifiable
  - No guarantee of receipt
- Standard phone calls
  - Interceptable
- Email
  - Interceptable
  - Email provider can (and does) read all of them

What IS secure

- Email
  - PGP (Pretty Good Privacy)
- Instant Messaging (with end-to-end encryption)
  - Open Source:: Pidgin, Adium, ChatSecure, Jitsi
  - Proprietary: WhatsApp, Signal, Telegram, iMessage, Threema (Swiss based)
- VOIP phone calls (with end-to-end encryption)
  - WhatsApp, Signal, Jitsi, Silent Phone, Zphone

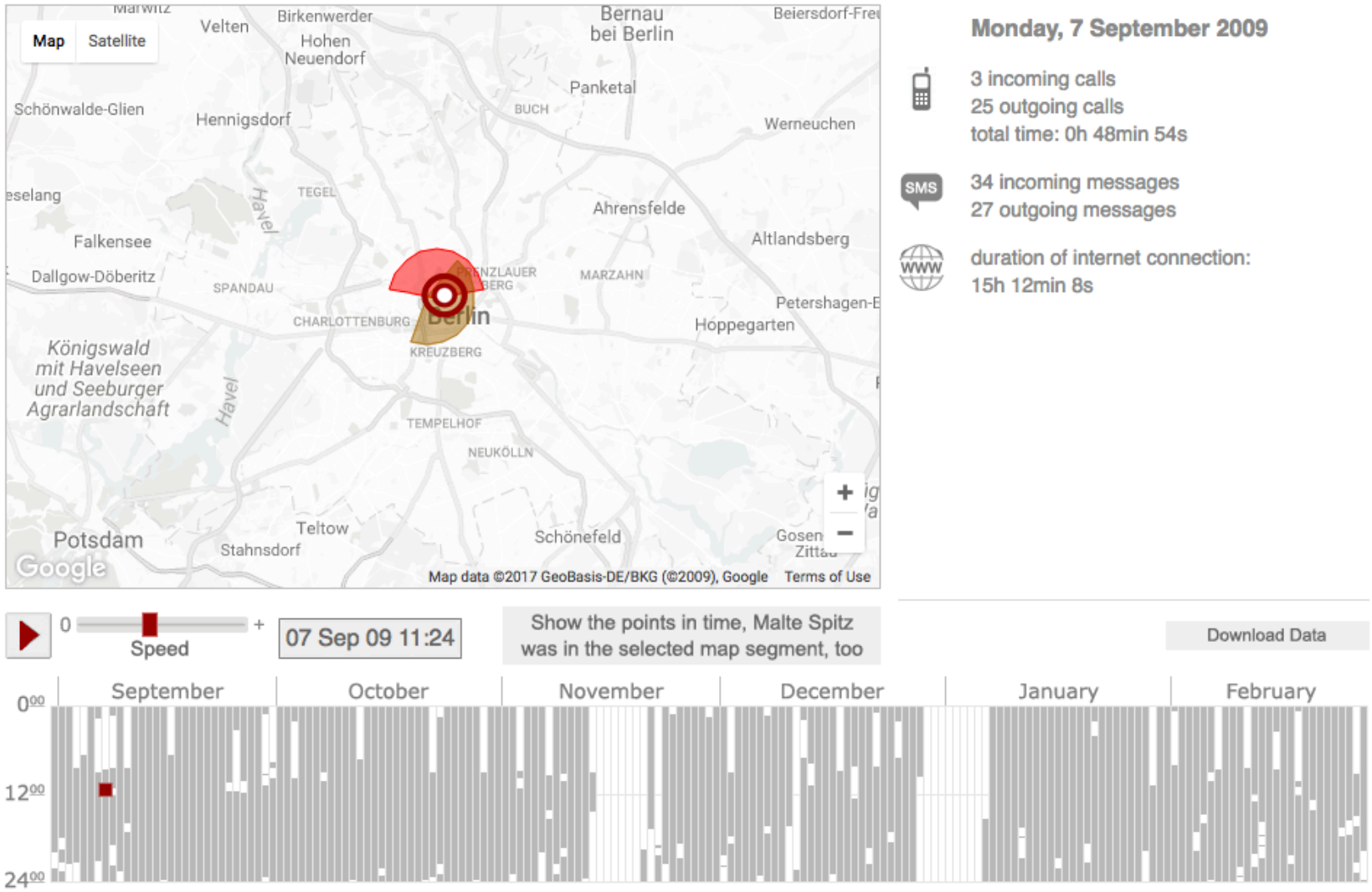
Group communication (in your team)

- Email
  - All on the same provider (data does not leave provider)
  - Choose HTTPS / TLS connections

- Group Chats
  - Self-hosted solutions: mattermost, let’s chat, rocket.chat

What is not protected by end-to-end encryption

- Recipients
- Frequency of communication
- Location of communication



http://www.zeit.de/datenschutz/malte-spitz-data-retention

Preventing Metadata Collection

- Tor
  - Used also to access the darkweb / darnket
  - Probably an overkill unless you are in places with social unrest

Mobile Security


BLUETOOTH SPEAKER
STAINED-GLASS DISPLAY
HOOK SHOT
GALLIUM CHASSIS
REMAINS SOLID UP TO 85°F
28-FACTOR AUTHENTICATION
SOUNDPROOF
CAN FEEL PAIN
LORAN NAVIGATION
E-ZPASS PARTNERSHIP:
PHONE CAN BE DROPPED INTO
COIN BASKET TO PAY TOLLS
60x OPTICAL ZOOM CAMERA
FOLDABLE (ONCE)
COT-CAUGHT MERGER SWITCH
SCREEN TRANSFERS IMAGES TO SKIN
IBM BUCKLING-SPRING HOME BUTTON
SQUELCH KNOB
RETINA STORAGE
SUPERCUTS PARTNERSHIP: TRIMS HAIR FED INTO CHARGING PORT
BACKGROUND TASK AUTOMATICALLY CATCHES AND EATS POKÉMON
INTRODUCING
THE XKCD PHONE 5
WE'RE TRYING TO CATCH UP TO APPLE BUT REFUSE TO SKIP NUMBERS®™

Misconception

Smartphones are less secure than computers

NO!

Smartphone Security

- Each application runs in its own sandbox
- Codebase is much smaller than that of regular operating systems
- UNIX based permissions system
- Devices are typically more up to date than computers
- Secure Enclaves / Trusted Computing is becoming more accessible to developers

IMPORTANT:

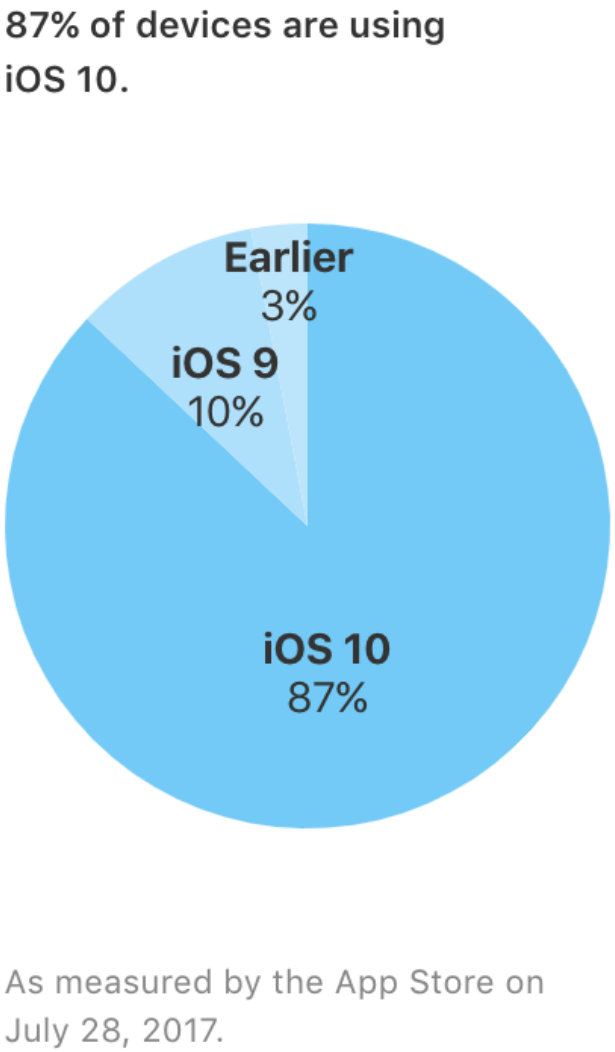
- Jailbreaking or Rooting one's device is the *worst security* practice

iOS Security (some details)

- Apple tests all applications (automated testing + manual testing)
- Only software signed by Apple can be installed
- Permissions are asked at runtime upon access to the resources
- Applications can store sensitive data in the system's keychain
- Keychain is unlocked *only* when the user enters the PIN-code or through fingerprint - Device reboot requires PIN code
- All files are encrypted on the device
- Fingerprints are stored in the *secure enclave*

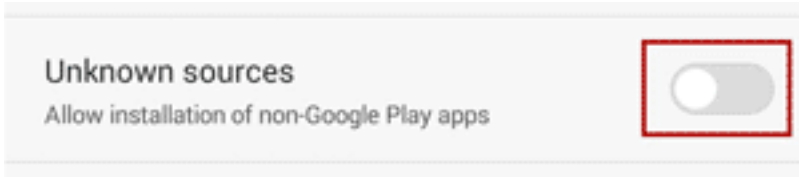
iOS Security (some details)

- Updates are pushed directly by Apple, best practice for security
- Release dates:
  - iOS 9: Sep'15
  - iOS 10: Sep'16



Android Security (some details)

- Applications go through automated tests (through an emulator) before acceptance
- User can disable critical security features



(disable this setting for security)

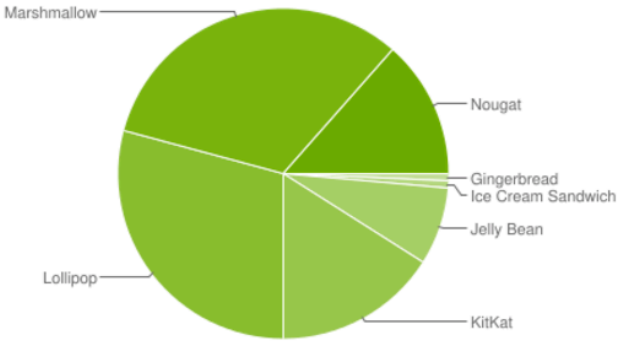
- Permissions are asked at install time (and at run-time, in newer versions of Android)
- Full disk encryption only available from some manufacturers (and only since Android 5.0)
- Screen lock via pattern less secure than longer PIN codes

Android Security (some details)

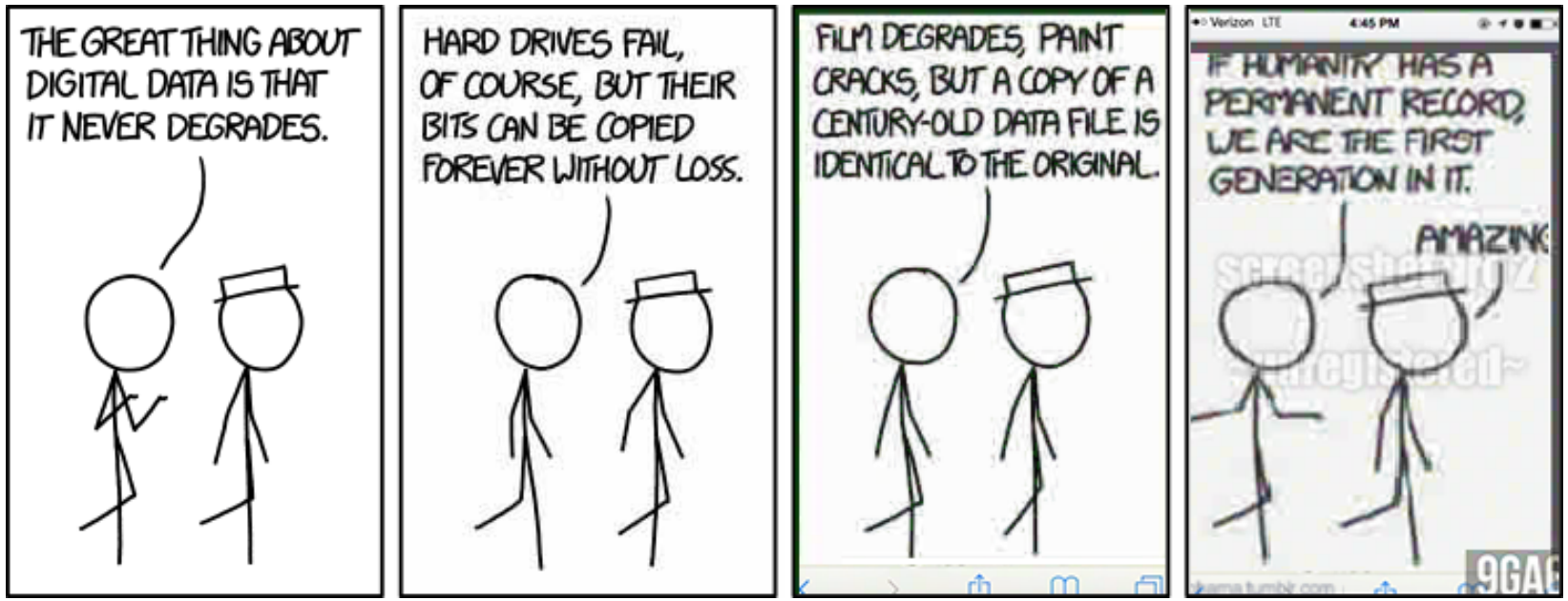
- Security landscape more variegated due to customizations and manufacturers not updating the main software promptly or dropping updates

	Version	Codename	API	Distribution
	2.3.3 - 2.3.7	Gingerbread	10	0.7%
	4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.7%
Jul'12	4.1.x	Jelly Bean	16	2.7%
	4.2.x		17	3.8%
	4.3		18	1.1%
Oct'13	4.4	KitKat	19	16.0%
Nov'14	5.0	Lollipop	21	7.4%
	5.1		22	21.8%
Oct'15	6.0	Marshmallow	23	32.3%
Aug'16	7.0	Nougat	24	12.3%
	7.1		25	1.2%

Data collected during a 7-day period ending on August 8, 2017.
Any versions with less than 0.1% distribution are not shown.



Data Storage


THE GREAT THING ABOUT DIGITAL DATA IS THAT IT NEVER DEGRADES.
HARD DRIVES FAIL, OF COURSE, BUT THEIR BITS CAN BE COPIED FOREVER WITHOUT LOSS.
FILM DEGRADES, PAINT CRACKS, BUT A COPY OF A CENTURY-OLD DATA FILE IS IDENTICAL TO THE ORIGINAL.
Verizon LTE
4:45 PM
IF HUMANITY HAS A PERMANENT RECORD, WE ARE THE FIRST GENERATION IN IT.
AMAZING
9GAG

File Storage and Sharing

- Mostly US-based
  - Terms and conditions might not be suitable for your business / sector
  - Data will be stored under US jurisdiction – check legal implications
  - Examples: Dropbox, Google Drive, box
- End-to-end encryption on the cloud: Tresorit
- Encryption for traditional file storage solutions: Boxcryptor
- Client-side encryption for files and self-hosting on your server: Seafile

Authentication and Malware

HACKERS RECENTLY LEAKED **153 MILLION** ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.

ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER PASSWORD		HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1
8babb6299e06eb6d		DUH
8babb6299e06eb6d	a0a2876eb1ea1fca	
8babb6299e06eb6d	85e9da81a8a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86da6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	eadec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE
39738b7adb0b8af7	617ab0277727ad85	SUGARLAND
1ab29ae86da6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279cadeb44	9dca1d79d4dec6d5	
38a7c9279cadeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279cadeb44		PURLOINED
a8ae5745a2b7af7a	9dca1d79d4dec6d5	FAV WATER-3 POKEMON

THE GREATEST CROSSWORD PUZZLE IN THE HISTORY OF THE WORLD

Passwords (Problem)

- Most common way to authenticate users
- Used to authenticate yourself to the many services you have
- Used by your users to authenticate to the services you offer
- Average user has many passwords:
  - (US) 130 - (UK) 118 - (FR) 95 - (Rest) 92
- **73%** of online accounts use **duplicated** passwords
- **54%** of people use **5** or less passwords in their whole life
- **> 3 billion** passwords have been **stolen** in the last 9 years
- Too easy to steal a user's password through phishing

Solutions

Password Manager

- Use a password manager
- Generate random passwords (30 characters and longer)
- Change the passwords of all your online accounts
- Examples:
  - 1Password
  - LastPass
  - KeePassX
  - Dashlane
- Use a strong master password or passphrase (it’s your last line of defense)

Solutions

Two Factor Authentication

- Two Factor Authentication (2FA) requires:
  - Something you know (the password)
  - Something you have (your mobile phone)
- Used for e-banking (via SMS or QR-codes)
- When available, enable 2FA
- Hands-off, flexible, Swiss made 2FA solution
  - Futurae 2FA suite is very easy to integrate in your software
  - Very competitive pricing model based on active user per month
  - Price per user ranging from CHF 1.- to CHF 0.02 depending on number of users

Malware / Virus / Spyware / Ransomware

- Installed by:
  - downloading malicious software online
  - opening an infected file or mail attachment
  - infected USB drives connected to the computer

- Run on your computer and have “unlimited” power:
  - Capture your keystrokes
  - Read your documents
  - Encrypt your files and demand for a ransom to decrypt them
  - Leak your private keys
  - Spread itself to all your contacts
  - Runs operations on behalf of the hacker

Solutions

Personal Computers (Generic Attacker)

- Prevention:
  - Antivirus (up to date)
  - Ad-blocker on your browser (e.g., uBlock Origin)
  - Do not open suspicious files sent to your e-mail

- Detection
  - Antivirus software
  - Malfunctioning system

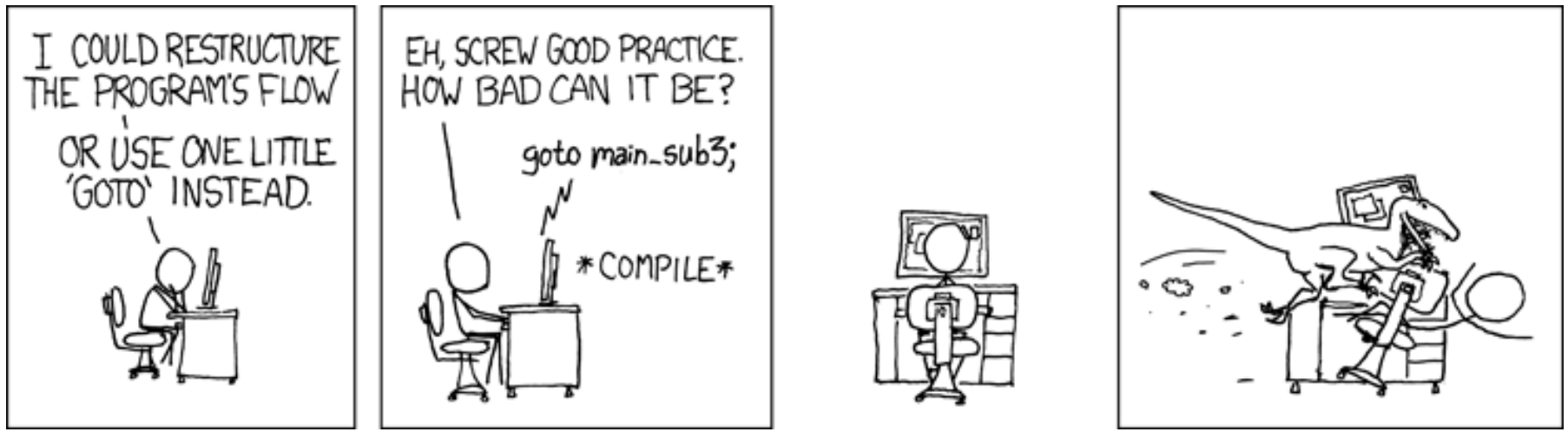
- Removal
  - Antivirus software
  - Instructions for specific type of malware

Solutions

Company-level (Targeted Attacker)

- Prevention:
  - Inform and train your employees
  - Run “test attacks” for training purposes
  - Block e-mails that contain potentially harmful attachments
    (Gmail has it enabled by default, enterprise-level solutions exist: Xorlab)
  - Keep computers and servers up to date with the latest security updates

IT Security Best Practices - Recap


I COULD RESTRUCTURE THE PROGRAM'S FLOW
OR USE ONE LITTLE 'GOTO' INSTEAD.
EH, SCREW GOOD PRACTICE. HOW BAD CAN IT BE?
goto main_sub3;
COMPILE

Take Away Slide

- Take IT Security seriously. It is a core business strength and important for your credibility.
- Keep software up to date
- Develop your services with care for security, not as an afterthought
- Use cryptographic tools in the right way
- Do not invent your own cryptography
- Consult experts early on (it is more cost effective)
- Use strong random passwords (use a password manager)
- Offer 2FA to your customers and employees
- Cloud-based deployments are *more* secure than on premise

Disclaimer

The content of this presentation is provided as is. Claudio Marforio or Futurae Technologies AG do **not accept** any **responsibility** or liability for the accuracy, content, completeness, legality, or reliability of the information contained herein.

Any third-party content is property of the respective author.