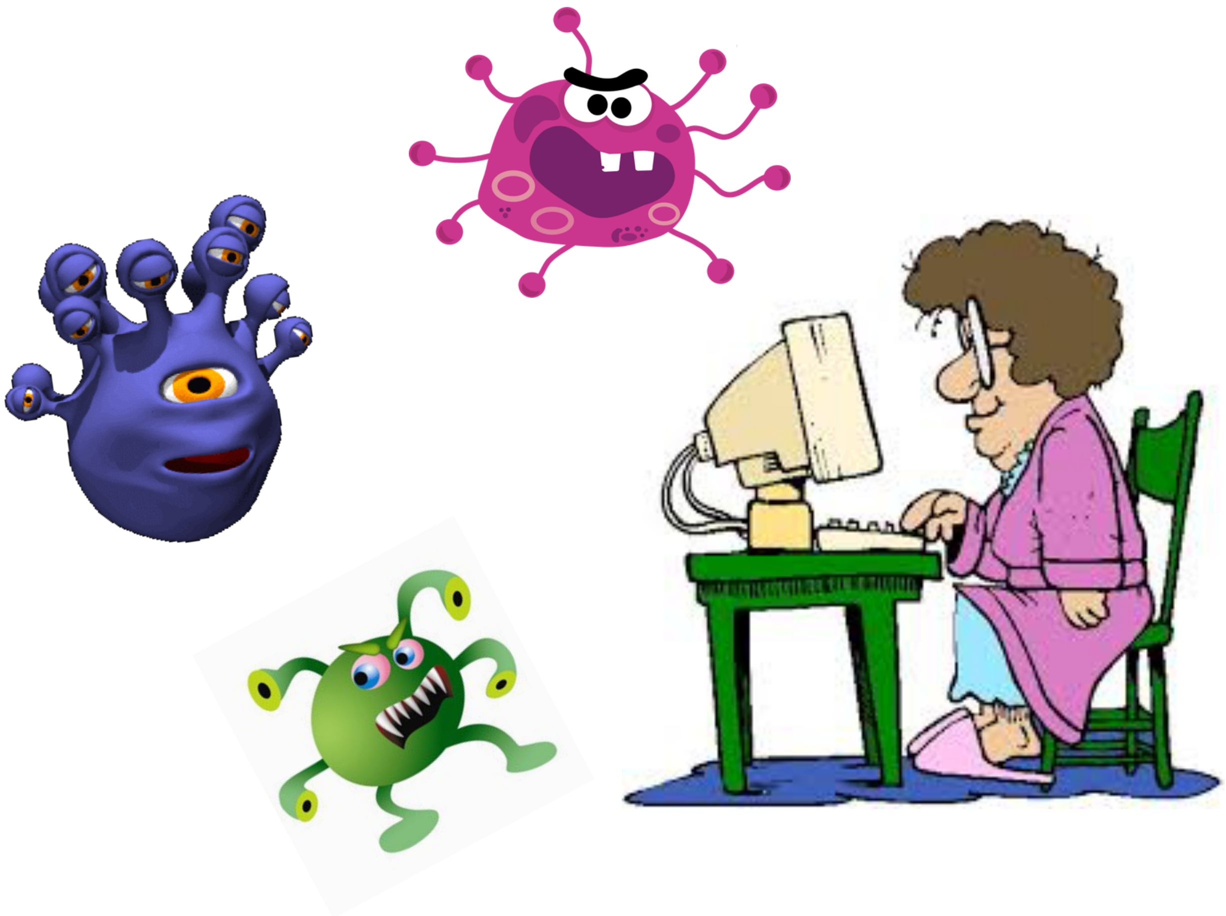
Security Engineering

Chester Rebeiro

IIT Madras

Security Engineering : What is it About?

Building systems that work even with adversaries



What does it involve?

- Threat assumptions
- Security goals
- Security policy
- Security Mechanism

Threat Assumptions

- Assumptions about the attacker
  - Is the attacker all powerful?

    (Theoretical; very difficult to achieve in practice)
  - What can the attacker do?

    (guess keywords; sniff keystrokes; co-resides on the same machine)
  - Is hardware untrusted?

    (Snowden revelations; hardware trojans; may need more assurance about the hardware)
  - Insider attackers

    (knowledge of the entire system architecture, security policies leaked)

Security Goals

Any security system must address the following goals

- Confidentiality
  keep data secret except to authorized users
- Integrity
  - prevent unauthorized users from making modifications
  - Prevent authorized users from making improper modifications
- Availability of data to unauthorized users
  - Handle Denial of Service, loss due to natural disasters, equipment failure

eg. Facebook

What does it involve?

- Security goals
- Security policy
- Security Mechanism
- Threat assumptions

CR

Security Policy

- Document that outlines the rules, laws, and practices so that security goals are achieved.
- High level statements generally signed by the company's CEO
  - Does not go into the technical details of how security goals are achieved

Security Policy for an IT Laboratory

- For a Lab security
- This is taken from https://www.sans.org/security-resources/policies/server-security/pdf/lab-security-policy
- Note the high level language, succent statements, and no details about how the the policy is implemented

Consensus Policy Resource Community

Lab Security Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

See Purpose.

2. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and <Company Name> networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at <Company Name> and its subsidiaries must adhere to this policy. This policy applies to <Company Name> owned and managed labs, including labs outside the corporate firewall (DMZ).

4. Policy

4.1 General Requirements

4.1.1 Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

4.1.2 Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard <Company Name> from security vulnerabilities.

4.1.3 Lab managers are responsible for the lab's compliance with all <Company Name> security policies.

4.1.4 The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

4.1.5 All user passwords must comply with <Company Name>'s *Password Policy*.

4.1.6 Individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).

4.1.7 PC-based lab computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

4.1.8 Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

4.1.9 No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

4.1.10 In accordance with *the Data Classification Policy*, information that is marked as <Company Name> Highly Confidential or <Company Name> Restricted is prohibited on lab equipment.

4.1.11 Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*

4.1.12 InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

4.2 Internal Lab Security Requirements

4.2.1 The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

4.2.2 The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

4.2.3 The Network Support Organization must record all lab IP addresses, which are routed within <Company Name> networks, in Enterprise Address Management database along with current contact information for that lab.

SANS **Consensus Policy Resource Community**

4.2.4 Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

4.2.5 All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

4.2.6 Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

4.2.7 Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-<Company Name> networks. These activities must be restricted within the lab.

4.2.8 Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

4.2.9 InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

4.2.10 Lab owned gateway devices are required to comply with all <Company Name> product security advisories and must authenticate against the Corporate Authentication servers.

4.2.11 The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with <Company Name>'s *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

4.2.12 In labs where non-<Company Name> personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no <Company Name> confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

4.2.13 Lab networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

4.3 DMZ Lab Security Requirements

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

What does it involve?

- Threat assumptions
- Security goals
- Security policy
- Security Mechanism

  Implementation aspects for the policy.
  (involves code, crypto, protocols, standards, …)

What's the Big Deal about Security Engineering?

- A security system should
  - Allow authorized users access to a resource
  - Disallow all other users access to the resource (in spite of users having supreme power, access to source code, etc.)

    (weakest link matters)

eg. Moodle
Assignment submissions should be accessible to all TAs → this is easily achieved
Assignment submissions should not be accessible to anyone but the Tas → not that easy!

CR

What can go wrong?

There can be mistakes in each of these

- Threat assumptions
- Security policy
- Security Mechanism

Messing up Security Policies

Forgot Password Security Questions

Not logged in Talk Contributions Create account Log

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages

Sarah Palin email hack

From Wikipedia, the free encyclopedia

The **Sarah Palin email hack** occurred on September 16, 2008, during the 2008 United States presidential election campaign when the Yahoo! personal email account of vice presidential candidate Sarah Palin was subjected to unauthorized access. The hacker, David Kernell, had obtained access to Palin's account by looking up biographical details such as her high school and birthdate and using Yahoo!'s account recovery for forgotten passwords. Kernell then posted several pages of Palin's email on 4chan's /b/ board. Kernell, who at the time of the offense was a 20-year-old college student, is the son of longtime Democratic state representative Mike Kernell of Memphis.

David Kernell

He was charged in October 2008 in federal court. After he was led into the court in leg irons and handcuffs, the judge released him on his own recognizance, pending trial.[1][2] The incident was ultimately prosecuted in a U.S. federal court as four felony crimes punishable by up to 50 years in federal prison.[3][4] The charges were three felonies: identity theft, wire fraud, and anticipatory obstruction of justice; and one optional as felony or misdemeanor: intentionally accessing an account without authorization. Kernell pleaded not guilty to all counts.

A jury trial, featuring the testimony of Sarah Palin and Bristol Palin, as well as 4chan founder Christopher Poole,[5] began on April 20, 2010.[3] On April 30, 2010, the jury found Kernell guilty on two counts: the felony of anticipatory obstruction of justice and the misdemeanor of unauthorized access to a computer.[6][7] Sarah Palin posted a note on her Facebook page stating that she and her family were thankful the jury had rendered a just verdict in her opinion.[8]

Kernell was sentenced on November 12, 2010, to one year plus a day in federal custody,[9] followed by three years of supervised release.[9] The sentencing judge recommended that the custody be served in a halfway house,[9] but the Federal Bureau of Prisons sent him instead to a minimum security prison.[10][11] In January 2012, the United States Court of Appeals for the Sixth Circuit found Kernell's awareness of a possible future FBI investigation was enough to uphold a conviction on obstruction of justice.[12]

Contents [hide]

https://en.wikipedia.org/wiki/Sarah_Palin_email_hack

Messing up Security Policies

When forgot password sends a “Reset Password” to a backup email address


HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

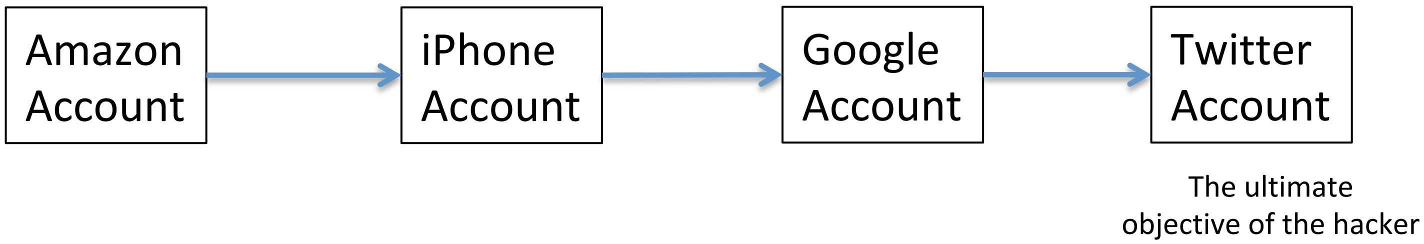
In a span of one hour

- Google account deleted
- Twitter account compromised
- AppleID broken into
- Remotely erased all data on iPhone, iPad, and MacBook

https://www.theverge.com/2012/8/6/3224597/mat-honan-hacked-apple-icloud-google-twitter

Hacked!

- Daisy Chained Accounts



The last 4 digits of the credit card

iPhone thought this was private information

Amazon thought this was public information

So you think you are safe with SMS OTP?

SMS-Based One-Time Passwords: Attacks and Defense
(Short Paper)

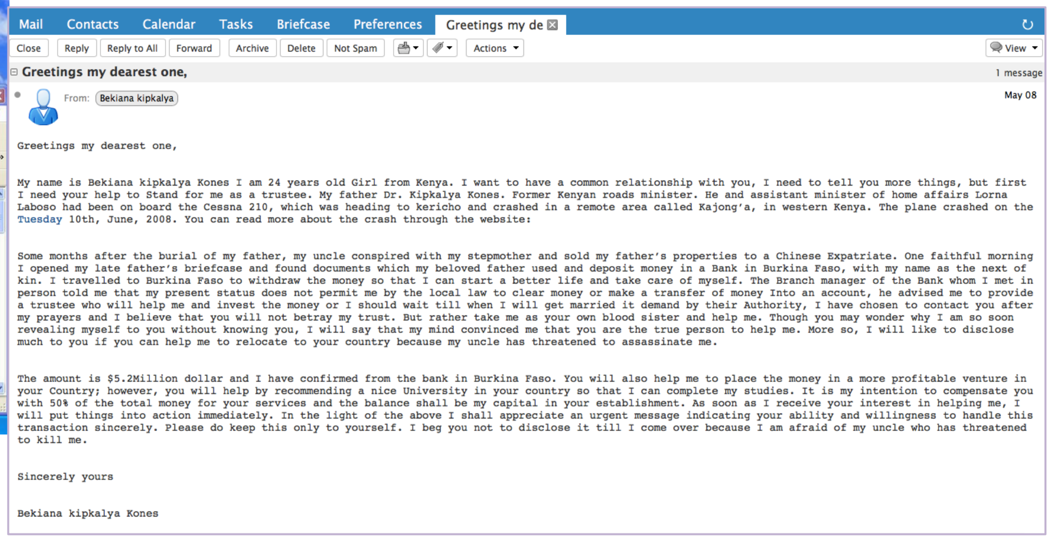
Collin Mulliner[1], Ravishankar Borgaonkar[2], Patrick Stewin[2], and Jean-Pierre Seifert[2]

[1] Northeastern University
crm@ccs.neu.edu
[2] Technische Universität Berlin
{ravii,patrickx,jpseifert}@sec.t-labs.tu-berlin.de

Abstract. *SMS-based One-Time Passwords* (SMS OTP) were introduced to counter phishing and other attacks against Internet services such as online banking. Today, SMS OTPs are commonly used for authentication and authorization for many different applications. Recently, SMS OTPs have come under heavy attack, especially by smartphone Trojans. In this paper, we analyze the security architecture of SMS OTP systems and study attacks that pose a threat to Internet-based authentication and authorization services. We determined that the two foundations SMS OTP is built on, cellular networks and mobile handsets, were completely different at the time when SMS OTP was designed and introduced. Throughout this work, we show why SMS OTP systems cannot be considered secure anymore. Based on our findings, we propose mechanisms to secure SMS OTPs against common attacks and specifically against smartphone Trojans.

Threat Assumptions (What can go wrong?)

- The human factor
  (can’t assume humans won’t fall prey to these)


Mail Contacts Calendar Tasks Briefcase Preferences Greetings my de

Close | Reply | Reply to All | Forward | Archive | Delete | Not Spam | Actions | View

Greetings my dearest one, — 1 message

From: Bekiana kipkalya — May 08

Greetings my dearest one,

My name is Bekiana kipkalya Kones I am 24 years old Girl from Kenya. I want to have a common relationship with you, I need to tell you more things, but first I need your help to Stand for me as a trustee. My father Dr. Kipkalya Kones. Former Kenyan roads minister. He and assistant minister of home affairs Lorna Laboso had been on board the Cessna 210, which was heading to kericho and crashed in a remote area called Kajong’a, in western Kenya. The plane crashed on the Tuesday 10th, June, 2008. You can read more about the crash through the website:

Some months after the burial of my father, my uncle conspired with my stepmother and sold my father’s properties to a Chinese Expatriate. One faithful morning I opened my late father’s briefcase and found documents which my beloved father used and deposit money in a Bank in Burkina Faso, with my name as the next of kin. I travelled to Burkina Faso to withdraw the money so that I can start a better life and take care of myself. The Branch manager of the Bank whom I met in person told me that my present status does not permit me by the local law to clear money or make a transfer of money Into an account, he advised me to provide a trustee who will help me and invest the money or I should wait till when I will get married it demand by their Authority, I have chosen to contact you after my prayers and I believe that you will not betray my trust. But rather take me as your own blood sister and help me. Though you may wonder why I am so soon revealing myself to you without knowing you, I will say that my mind convinced me that you are the true person to help me. More so, I will like to disclose much to you if you can help me to relocate to your country because my uncle has threatened to assassinate me.

The amount is $5.2Million dollar and I have confirmed from the bank in Burkina Faso. You will also help me to place the money in a more profitable venture in your Country; however, you will help by recommending a nice University in your country so that I can complete my studies. It is my intention to compensate you with 50% of the total money for your services and the balance shall be my capital in your establishment. As soon as I receive your interest in helping me, I will put things into action immediately. In the light of the above I shall appreciate an urgent message indicating your ability and willingness to handle this transaction sincerely. Please do keep this only to yourself. I beg you not to disclose it till I come over because I am afraid of my uncle who has threatened to kill me.

Sincerely yours

Bekiana kipkalya Kones

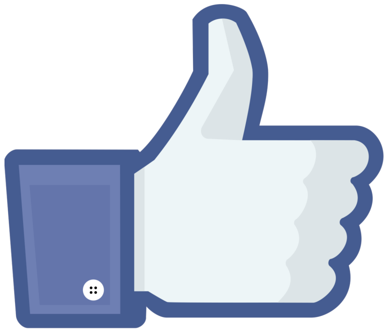
Threat Assumptions (What can go wrong?)

- Threat model change with time

1980s

Kerberos, invented in 1980s, used DES with 56 bit keys for encryption

56 bit keys pretty safe in the 80s.

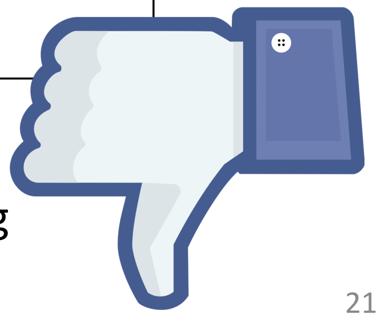


1990s

Kerberos, invented in 1990s, **still** used DES with 56 bit keys for encryption

56 bit keys cannot be practically broken in the 90s in a single day (with specialized hardware)

DES went obsolete, but nobody thought of changing Kerberos

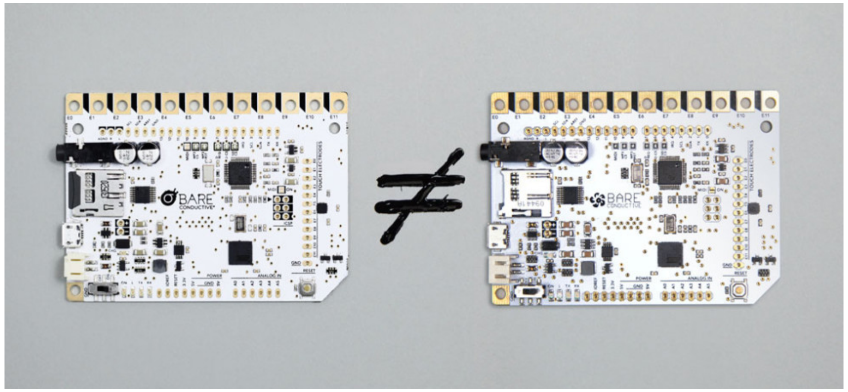


Threat Assumptions (What can go wrong?)

- Hardware Backdoors / Cloned Hardwre

  Do you need to Worry about Cloned Hardware?

Hardware backdoors



Cannot assume your hardware is safe

Threat Assumptions (what can go wrong?)

- **Trusted parties may get compromised**

- Example : DigiNotar (a Dutch Certifying Authority) compromised in 2011.
  - Issued fraudulent certificates

    which were used to conduct man-in-the-middle attacks against Google, Yahoo, Mozilla, and many other services
  - Targeted 300,000 gmail users
  - Suspected to be work of a Government

Threat Assumptions (What can go wrong?)

- Improper use of crypto

- Suppose the prime generation for RSA was faulty
  - So that, primes generated were always from a small subset
  - Then, RSA can be broken
- Pairwise GCD of over a million RSA modulii collected from the Internet showed that
  - 2 in 1000 have a common prime factor

Ron was Wrong, Whit is right, 2012

Threat Assumptions (What can go wrong?)

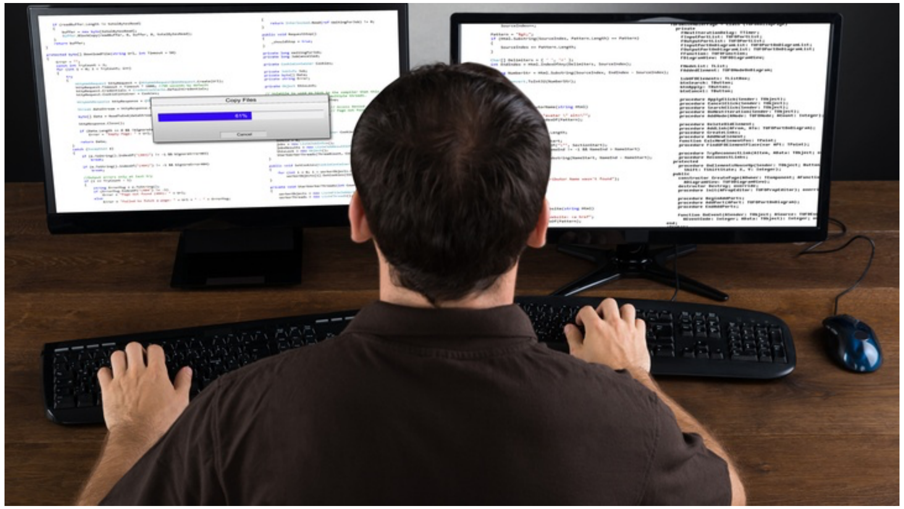
- Insiders cannot be trusted

1980s had an insider inserting backdoors in a secure OS used for military applications

the attacker could get access to the system through the backdoor

Security Mechanisms (What can go wrong?)

- Due to Programmers
  - Forget
  - Don't know
  - Only look for functional correctness
- Programming Languages
  - Do not inherently do certain checks



Number of Password Attempts

Websites typically have N password attempts before your account is blocked

Passwords are not very difficult to crack
(see John the Ripper : http://www.openwall.com/john/)
combined with the fact that many people are not very smart at setting passwords
(one of the most famous passwords is password)
(http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using)

What happens if the programmer forgets to do the count check?
Disaster any time

Number of Password Attempts

Apple's iCloud password-guessing rate limits

The iCloud has many services and many APIs.

One service forgot to implement limiting the no. of password trials.

Adversary could try infinite times

CR https://github.com/hackappcom/ibrute

Missing Access Control Checks

Citi bank data breach in 2011

Citi's Login Page

Enters username and password
LOGIN

→

Webpage 2

The URL contains the account number of the user

Change the account number in this page and you will get another user's account details

http://www.nytimes.com/2011/06/14/technology/14security.html

Seeding the Random Number Generator

- Random numbers generated by PRSG
- PRSG needs to be fed an initial value called seed.
- If the seed are equal, the random numbers generated are the same.

Bitcoin Theft

- Random numbers used to generate secret keys and make Bitcoin transactions
- If an attacker steals the random number, bitcoins are stolen
- Android's Java SecureRandom API forgot to seed the PRSG in certain cases. Seed was initialized to 0.
  Random numbers can be then predicted,
  keys can then be stolen

https://bitcoin.org/en/alert/2013-08-11-android

Program Bugs That Can be Exploited (Most Common Vulnerability)

- Buffer overflows
  - In the stack
  - In the heap
  - Return-to-libc attacks
- Double frees
- Integer overflows
- Format string bugs

CR