COM-402
Information Security and Privacy

Course Introduction and Basic Concepts

(slide credits: Linus Gasser, Ceyhun Alp, Sandra Siby, Cristina Basescu, Bryan Ford)
Lecture 1: Course introduction

- **Course logistics**
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview

- **Course overview**
  - How and what information is sensitive?
  - Threats: what can go wrong?
  - Data encryption and anonymization
  - User management (access control, authentication) & Operational security
  - Machine learning security and privacy
  - Blockchains and smart contracts
  - Many others
Important course sites and tools

● Moodle for COM-402
  ○ Announcements and discussion forum
  ○ Slides, exercises, solutions
  ○ Project descriptions

● SpeakUp
  ○ [https://goo.gl/4T5OB7](https://goo.gl/4T5OB7)
  ○ Questions/comments during class

● Clicker
  ○ [http://clickers.epfl.ch/students](http://clickers.epfl.ch/students)
  ○ Respond to poll-style questions during class
  ○ Only mobile apps
## Tentative Course Syllabus

<table>
<thead>
<tr>
<th>Date</th>
<th>Content</th>
<th>Date</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.02</td>
<td>Course introduction and basic concepts</td>
<td>17.04</td>
<td>Security policy and regulation</td>
</tr>
<tr>
<td>27.02</td>
<td>Common threats</td>
<td>24.04</td>
<td>Anonymization and de-anonymization</td>
</tr>
<tr>
<td>06.03</td>
<td>Crypto basics</td>
<td>01.05</td>
<td>Machine learning security &amp; privacy</td>
</tr>
<tr>
<td>13.03</td>
<td>Database security</td>
<td>08.05</td>
<td>Advanced privacy techniques</td>
</tr>
<tr>
<td>20.03</td>
<td>Personally identifying information (PII)</td>
<td>15.05</td>
<td>Blockchains &amp; smart contracts</td>
</tr>
<tr>
<td>27.03</td>
<td>User management</td>
<td>22.05</td>
<td>Side-channel attacks/defenses</td>
</tr>
<tr>
<td>10.04</td>
<td>Network security: detection / response</td>
<td>29.05</td>
<td>What's hot in security research</td>
</tr>
</tbody>
</table>
Contact information

**Lecture instructors:**

- Bryan Ford - bryan.ford@epfl.ch - BC210
- Linus Gasser - linus.gasser@epfl.ch - BC208

**Teaching assistants:**

- Cristina Basescu - cristina.basescu@epfl.ch - BC263
- Kirill Nikitin - kirill.nikitin@epfl.ch - BC209
- Sandra Siby - sandra.siby@epfl.ch - INR015
- Ceyhun Alp - enis.alp@epfl.ch - INR012
- Raphaël Dunant - raphael.dunant@epfl.ch
Exercises and grading

● **Weekly workload**
  ○ Lectures: 2h - Tuesdays 4:15pm in CM1
  ○ Exercises: 2h - Fridays 3:15pm in CM3
  ○ Homework: 5-10h / week

● **Grading structure:**
  ○ Exercises: approx 40% of grade, lowest-scoring homework dropped
  ○ Final exam: approx 60% of grade
Programming Exercises Overview

- **Six exercise sets over the semester (approx every 2 weeks)**
- **Friday group exercise sessions (3:15pm-5pm CM3)**
  - Introduce tools to be used in assignments (e.g., Docker, WireShark, etc.)
  - Introduce programming assignments
  - Practice, walk through example problems in group context
  - Answer questions and help with use of tools
- **Main problem-solving and programming to be done “on your own”**
  - For each assignment we will provide a Docker container to start with
  - You will need to install and run on your preferred laptop/desktop
    - You will use programming tools provided in container (Python, JavaScript, SQL)
    - You can use native host editors, IDEs, etc., via Docker shared directories
  - Many problems require you to obtain a token for an all-or-nothing grade for that problem
Programming Exercise Outline

<table>
<thead>
<tr>
<th>Set</th>
<th>Type</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attack</td>
<td>Hacking 101: sniffing networks; exploiting bugs and humans</td>
</tr>
<tr>
<td>2</td>
<td>Defense</td>
<td>Basic encryption and security-hardening practices</td>
</tr>
<tr>
<td>3</td>
<td>Attack</td>
<td>Database-centric attacks: SQL injection, credential databases</td>
</tr>
<tr>
<td>4</td>
<td>Defense</td>
<td>Better database hardening, naive anonymization</td>
</tr>
<tr>
<td>5</td>
<td>Attack</td>
<td>De-anonymization via correlation (e.g., “Netflix attack”)</td>
</tr>
<tr>
<td>6</td>
<td>Defense</td>
<td>Differential privacy and anti-correlation techniques</td>
</tr>
</tbody>
</table>
What fun data can a malicious network operator or cyber-cafe lurker get unauthorized access to?
Attack/defense hw3&4 - database security

https://xkcd.com/327/
Attack/defense hw5&6 - Data privacy, anonymization

DOGBERT CONSULTS

CUSTOMER DATA IS AN ASSET THAT YOU CAN SELL.

IT'S TOTALLY ETHICAL BECAUSE OUR CUSTOMERS WOULD DO THE SAME THING TO US IF THEY COULD.

IN PHASE ONE, WE'LL DEHUMANIZE THE ENEMY BY CALLING THEM "DATA."

Dilbert.com
DilbertCartoonist@gmail.com

© 2010 Scott Adams, Inc. Dist. by UFS, Inc.
Lecture 1: Course introduction

● Course logistics
  ○ Course web sites and tools
  ○ Tentative schedule and topic outline
  ○ Programming exercises overview

● Course overview
  ○ How and what information is sensitive?
  ○ Threats: what can go wrong?
  ○ Data encryption and anonymization
  ○ User management (access control, authentication) & Operational security
  ○ Machine learning security and privacy
  ○ Blockchains and smart contracts
  ○ Many others
Information Sensitivity

Many types of information -> many kinds and levels of *sensitivity*

- What might happen, and how bad, if “the wrong person” gets information?

Example: photos inside home “more sensitive” than photos taken in public park

- But what if taken with long-distance telephoto aimed at bedroom window?
Sensitivity can depend on Context

Information sensitivity often depends on context

- You may be perfectly comfortable with your friends seeing party photos...
- But may be harmful if seen by future employer (or border control)...

![Cartoon of a boss saying, "Forget the resume, son. Let's just take a look at what you have posted on your Facebook instead." The employee looks concerned.]
Sensitivity can depend on Longevity

- **Ephemeral, rapidly-changing, automatically-collected data**
  - Mobile cell tower logs, security cameras, website visit logs, …
  - Each data point typically not very sensitive by itself, but more sensitive in aggregate (user profiling) and/or at particular times (clinic visit)

- **Information actively provided by users**
  - E-mail, phone calls, chat logs, social media comments, online purchases & reviews
  - Sensitivity in principle governed by awareness & consent … but many surprises lurking

- **Slowly-changing or difficult-to-change information**
  - Social security number, AHV-number, passport-number
  - Sensitive in part because difficult to recover when breached

- **Practically unchangeable information, e.g., biometrics**
  - Fingerprints, DNA, ‘Omics and other medical data
  - Can’t change your DNA if breached, *and* can also breach privacy of your relatives…
Lecture 2: Common Threats

Examples of things that can go wrong (and have)

- **Data breaches:** when hackers get in and grab sensitive data
  - US Office of Personnel Management (OPM): 21.5 million security clearance records
  - Swiss RUAG: long-term, well-maintained malware infection over several years

- **De-anonymization:** when “anonymized” datasets are sensitive after all
  - Netflix Prize dataset: de-anonymized by correlating with IMDB film reviews

- **Ransomware:** pay to decrypt your own data
  - 10+ US hospitals infected in 2016, one paid $17,000

- **Phishing:** acquire credentials to break into business, personal accounts
  - Identity theft, or stepping-stone into employee’s organization
Why the OPM Hack Is Far Worse Than You Imagine

By Michael Adams  Friday, March 11, 2016, 10:00 AM

The Office of Personnel Management ("OPM") data breach involves the greatest theft of sensitive personnel data in history. But, to date, neither the scope nor scale of the breach, nor its significance, nor the inadequate and even self-defeating response has been fully aired.

The scale of the OPM breach is larger and more harmful than appreciated, the response to it has worsened the data security of affected individuals, and the government has inadequately addressed the breach’s counterintelligence consequences. While we can never know for sure exactly what the government is doing in secret to address the breach and mitigate its consequences, based on what is publicly known, the millions affected by the breach have good reason to fear.

Below, I explore the scale of the problem.
Paper claims special forces unit exposed by hack

By Jeannie Wurz

The identities of members of an elite Swiss special forces army unit may have been revealed in a hack of the RUAG defence contractor, according to the NZZ am Sonntag newspaper.

On Sunday, the NZZ am Sonntag reported that Russian IT specialists had gained access to personal data of members of the secret DRA10 special forces unit, which was established for risky operations in foreign countries.

“We're racking our brains trying to determine whether the elite soldiers will have to be given new identities,” an insider told the newspaper.

According to a press statement released by the Defence Ministry on Wednesday, the government works closely with defence contractor RUAG, whose IT system was the target of the attacks.
WHY HOSPITALS ARE THE PERCENT TARGETS FOR RANSOMWARE

RANSOMWARE HAS BEEN an Internet scourge for more than a decade, but only recently has it made mainstream media headlines. That’s primarily due to a new trend in ransomware attacks: the targeting of hospitals and other healthcare facilities.
Who all might present a “threat”?

Many threat models, often with different levels of budget & capability

- **Random people: friends, partners, journalists, competitors, trolls**
  - Attack: domestic spying, “spouseware”

- **Crooks: theft, ransom, blackmail**
  - Attack: E-mail phishing
  - Attack: Microsoft chatbot Tay
  - Attack: The DAO

- **State agencies: law enforcement, espionage, tax office**
  - Attack: Stuxnet
  - Attack: Apple-FBI
This Gmail Phishing Attack Is Fooling Even Savvy Users

Lee Mathews, CONTRIBUTOR
Observe, ponder, and writing about tech. Generally in that order. FULL BIO
Opinions expressed by Forbes Contributors are their own.

There's a new phishing campaign targeting Gmail users. Security researchers say that it's highly effective and that even experienced, tech-savvy users are being tricked by it.

Whoever is behind this campaign is either employing a team that's ready to pounce on newly-compromised accounts or their code includes some fairly sophisticated automation features. As soon as a victim submits a password, the criminals log in to the victim's Gmail account.
Lecture 3: Cryptography Basics

- Cryptography is an essential toolbox for many security mechanisms
  - Secure communication (e.g., HTTPS, SSH, GSM)
  - File & disk encryption (e.g., VeraCrypt, GPG)

- Goals
  - Confidentiality
  - Integrity
  - Authentication

- Achieve these goals using various tools
  - Symmetric (private-key) encryption
  - Asymmetric (public-key) encryption
  - Cryptographic hash functions
  - Public key infrastructure (PKI)
Encryption: Making Data Unintelligible

Keep information private while stored or communicated via non-private channels

- Modern encryption relies on *keys*
- Even with full knowledge of *algorithm*, only holder of correct *key* can decrypt
Encryption At Rest

Encrypted hard disk partitions, databases, folders

- Protect from some attacks: e.g., stolen laptop or phone
  - Provided device was turned off or locked when stolen
  - Provided password isn’t easily guessable, encryption software not readily crackable, …

- Who holds the encryption keys?
  - User device? If device is stolen, thief can use it to break into a lot more
  - Central database? If server breached, hacker can get into many users’ accounts

- What if a key is lost/misplaced/forgotten?
  - With “strong” encryption, losing a key means there is no way to recover data
  - If there is a “legit” way to recover a key, an attacker or spy might do the same

- What happens when sending the data to another server?
Encryption in Transit

How to get data securely between user and server, between company sites?

- Between data warehouses
  - NSA-attack on Google

- Between user and web sites, E-mail servers, etc.
  - HTTP - TLS
  - SMTP - TLS

- Between users: encrypted E-mail, encrypted chat
  - Skype - not sure what the protection is - probably opened to government inquiries
  - WhatsApp - relies on secure protocol, but has some user-friendly downgrades
  - Signal - open source, highly security-conscious, but still known weaknesses
Current Efforts - Google

GFE = Google Front End Server
SSL Added and Removed here!
Traffic in clear text here.

GFE = Google Front End Server
SSL Added and Removed here!
Traffic in clear text here.
The Challenges of “Usable Encryption”

Will typical users really understand…

What the encryption icons mean

When you're sending or receiving messages, you can see the level of encryption a message has. The color of the icon will change based on the level of encryption.

- **Green (S/MIME enhanced encryption) 🚨**: Suitable for your most sensitive information. Gmail uses S/MIME to encrypt all outgoing messages if we have the recipient's public key. Only the recipient with the corresponding private key can decrypt this message.

- **Gray (TLS - standard encryption) 🔒**: Suitable for most messages. TLS (Transport Layer Security) is used for messages exchanged with other email services who don't support S/MIME.

- **Red (no encryption) 📥**: Unencrypted mail which is not secure. Gmail uses past messages sent to the recipient's domain to predict whether the message you’re sending won’t be reliably encrypted.
The Challenges of “Usable Encryption”

...let alone what it means and what to do if something goes wrong?
Lecture 4: Database Security

- Databases are used everywhere
  - Banking, industry, government, social media, etc.
  - Leads to new types of analysis (e.g., big data, machine learning)

- Critical to think about its security
  - Security requirements
  - Main attack vectors
  - Main protections

- Some issues:
  - Access control (authenticating users and their rights)
  - Input validation & SQL injections
  - Protection of the sensitive data (passwords, credit card info, medical records, etc.)
Lecture 5: Personally Identifiable Information

- What is personally identifiable information (PII)?
  - Both sensitive and nonsensitive information
  - Has value for third parties

- Nonsensitive data can become sensitive by combining different sources
  - Co-location and position information
  - De-anonymization of databases (e.g., Netflix deanonymization)

- Management concepts
  - How to collect the data and operate on it

- Legislation around the world
Lecture 6: User and Access Management

- **Access control**
  - Role-based access control
  - Discretionary access control
  - Mandatory access control

- **Authentication**
  - Passwords
  - Kerberos - network authentication protocol from MIT
  - Multi-factor authentication
    - One-time passwords
    - Biometrics
  - LDAP

- **How to stay safe online?**
  - Training the weakest link in the system (aka the users!)
Access Control

Access control is a mechanism defining who *should* have access to information

- **Who?**
  - Might be specified by individual: Alice, Bob, Charlie, Dave, …
  - Might be specified by group/role: Doctors, Board Members, Accounting, …

- **What?**
  - Access to one document, a whole folder/tree
  - Access to perform certain queries on a database

- **How?**

- **When?**
  - Is granted access indefinite, or does it end at a particular time (Dec 31)
  - or at occurrence of a particular event (revocation, employment termination)?
Authentication of Users

How does Alice prove she’s Alice (e.g., to obtain access to information)?

- **Simple username (e.g., IRC)**
  - No security, anyone can be “Alice”

- **Typical: username + password (most Web accounts)**
  - Security relies completely on “something you know” (password)

- **Two factor Authentication (2FA): username + password + token**
  - Combination of “something you know” (password) plus “something you have” (token)

- **Device-centric authentication**
  - Web persistent login, SSH public key login, Kerberos file sharing
Two-factor authentication ("2FA")

There are 3 common ways to use 2FA:

1. **SMS**
   - I'd like to login
   - I've sent you an SMS with a code. Enter the code to finish logging in.
   - Problems: Your phone # can get stolen (this happens in real life!)
   - Sometimes SMS doesn't arrive

2. **Google Authenticator app**
   - I'd like to login
   - Enter the code from that app on your phone
   - Problems: These codes can still be phished.

3. **Security key**
   - I'd like to login
   - *Tap yubikey*
   - *Done*
   - Problems: You have to buy it
   - Not every website has support

I have a really secure email password?

That's awesome!! but you know, if a hacker got my password, they STILL can't get into my email 😕.
Authentication of Remote Servers and Users

Authenticating servers is just as critical as authenticating users:
How does Alice know she’s connecting to the real “google.com”?

- Many attacks (phishing) rely on tricking the user into trusting a fake version of an otherwise-uncompromised service
  - Alice enters her username+password; hacker captures and uses them
- Public Key Infrastructure (PKI) Certificates
  - Chain of Certificate Authorities (CAs) attest to correct ownership of “google.com”
- Peer-to-peer authentication: PGP keys, SSH fingerprints, Signal verification
  - Peer users supposed to verify in-person or out-of-band… (but how often do they?)
Lecture 7: Network and Operational Security Practices

Set of practices for identifying threats and minimizing risks of compromise

- **Identify the risk**
  - Know your network
  - Update the information regularly
  - Evaluate what information is valuable

- **Minimize the risk**
  - Compartmentalization (access control, separation of data)
  - Protection on network level
  - Backup

- **Prepare response**
  - Have a plan what to do
  - Save logs in case of an attack
Connectivity

Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals

The rise of malware that holds data hostage has led companies to buy in to using ransomware as an alternative to traditional forensic techniques.

by Tanya Kibler  |  June 2015

Digital currency has been variously promoted as a hedge against inflation, a gateway to make international transactions easier, and a feature of e-commerce. A new research suggests that companies are now stockpiling Bitcoin for a different reason: so they can pay up quickly if their data is held ransom by malicious software.

Ransomware, as it is called, has locked up the data of huge numbers of individuals and businesses in recent years. Many of them, including police departments and hospitals, have opted to pay up to get their data back.
RUAG response - not prepared
Compartmentalization

General principle: limit potential damage of breaching any one component

- Principle of least-privilege, “need-to-know”
- Networks: isolate “zones” with different functions, access
- Operating systems, virtual machines: isolate different users, apps, guests
Lecture 8: Security/Privacy Policy

● What incentives do companies have to implement security measures in their products and processes?

● Policy approaches for better security
  ○ Standardized algorithms, licensing
  ○ Independent authorities to evaluate products
  ○ Legal liability for failures

● Privacy vs the State: Should governments be allowed to access personal data?
  ○ Individuals’ rights to privacy vs the government’s duty to provide safety against criminals etc.

● Data protection laws vary across countries
  ○ Comparison between laws in the US and Europe

● Privacy and Online Speech
  ○ Can we provide freedom of speech but also protection against abuse and trolling?
Is it possible to “scrub” sensitive information from data?

- Often to make it available to the public, and/or to researchers
Anonymization failures

Sensitive data, but with “no names”: e.g., medical data, Netflix history

Separate “auxiliary information”: e.g., voter registration, IMDB reviews

- Ethnicity
- Visit date
- Diagnosis
- Procedure
- Charge
- Zip
- Birthdate
- Sex
- Name
- Address
- Party affiliation
- Date registered
- Date last voted
Lecture 10: Machine Learning Security & Privacy

- **ML is becoming ubiquitous**
  - Data security, Financial trading, Healthcare, Marketing personalization, Fraud detection, Recommendations

- **The dark sides of ML: are algorithms “fair”?**
  - Algorithmic bias: Google ads

- **Attacking and defending ML**
  - Cause AI to make mistakes
  - Membership inference attacks against black-box models
Twitter taught Microsoft’s AI chatbot to be a racist asshole in less than a day

by James Vincent | @jvincent | Mar 24, 2016, 6:43am EDT

It took less than 24 hours for Twitter to corrupt an innocent AI chatbot. Yesterday, Microsoft unveiled Tay — a Twitter bot that the company described as an experiment in “conversational understanding.” The more you chat with Tay, said Microsoft, the smarter it gets, learning to engage people through “casual and playful conversation.”
Lecture 11: Advanced Privacy Topics

- Crypto from the users’ perspective
  - Examples: Electronic voting, Electronic auctions, Electronic cash schemes, Contract signing, Anonymous transactions
  - Enable parties to carry out distributed computing tasks in a secure manner
  - An attacker may try to alter the results
  - Different adversary types, e.g., honest-but-curious

- Secure multi-party computation
  - Examples: Electronic voting, Electronic auctions, Electronic cash schemes, Contract signing, Anonymous transactions
  - Enable parties to carry out distributed computing tasks in a secure manner
  - An attacker may try to alter the results
  - Different adversary types, e.g., honest-but-curious

- Privacy and cloud computing
  - Control privacy of data stored in the cloud
  - Private information retrieval
  - Oblivious RAM
  - Privacy vs overhead
Lecture 12: Blockchains & Smart Contracts

- **Redundancy and fault tolerance**
  - The CAP theorem: Consistency, Availability, Partitions

- **Consensus & Byzantine failures**
  - Properties: validity, agreement, termination, integrity

- **Bitcoin & blockchains**
  - Conflict resolution through leader election (proof of work)
  - Unstable consensus (forks): risk or wait?
  - Double-spending attacks

- **Smart contracts**
  - User-defined programs running on top of blockchains
  - Ethereum
Lecture 13: Side-Channel Attacks and Defenses

● Embedded applications are on the rise
  ○ RFID, Sensor networks, “Internet of Things”
  ○ Hardware-implemented crypto often shows severe vulnerabilities

● Side-channel attacks target crypto implementations
  ○ How much power the computer uses: triple DES power analysis
  ○ How long computation cases take

● Prevention
  ○ Example: Avoid conditional branch and secret intermediates
  ○ Using XOR, OR etc operations instead of IF / ELSE
  ○ Takes the same amount of time *and* power
Conclusion

● **This Wednesday (tomorrow!) on Moodle**
  ○ Instructions on setting up homework tools
  ○ First homework online

● **This Friday**
  ○ First exercise session
  ○ First homework Q & A

● **Next Tuesday**
  ○ More on common threats

Thanks for coming!