Lecture 5

More on perfect secrecy

Nicola Laurenti October 14, 2020

Lecture 5— Contents

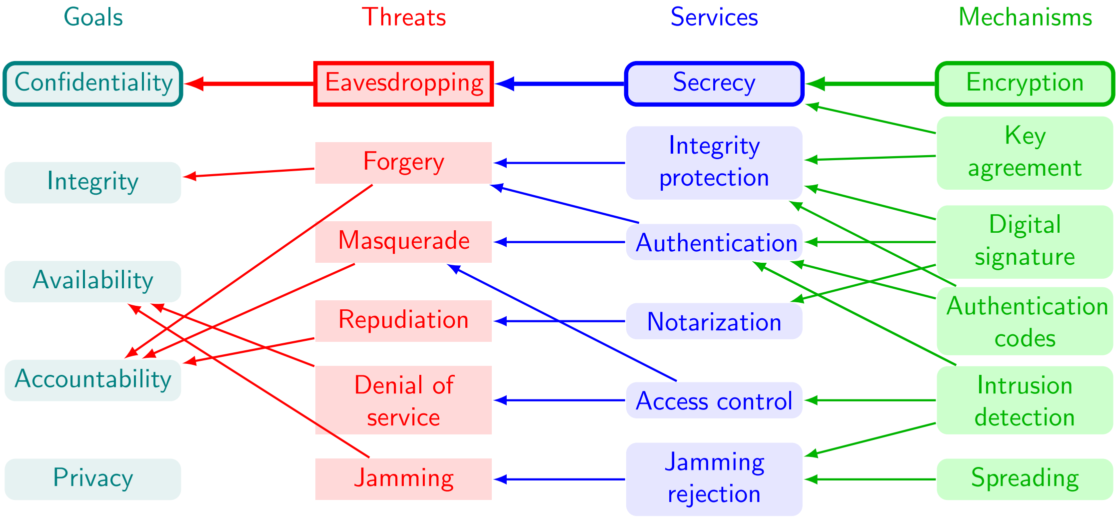
Review of basic Information Theory notions

The price of perfect secrecy

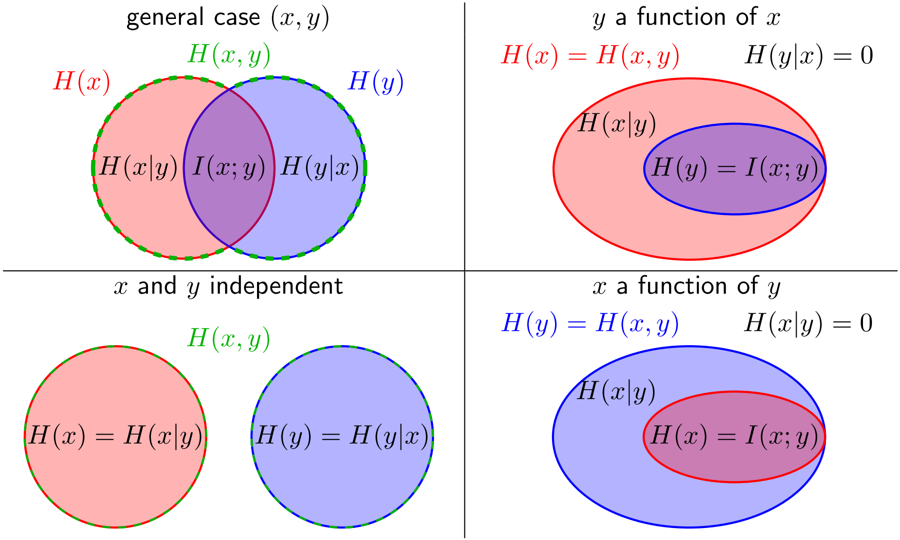
- Necessary condition
- Unconditional secrecy

Classificaton of attacks

Security goals, threats, services and mechanisms



Visualization of entropy relationships



Chain rules for (conditional) entropy

Some basic properties of entropy:

1. $H(x, z) \geq H(x)$
2. $H(x|z) \leq H(x)$
3. $H(x, z) = H(x|z) + H(z)$

They can be generalized to any collection of rvs $x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_\ell$ as the following chain rules:

1. $H(x_1, \ldots, x_n, z_1, \ldots, z_\ell | y_1, \ldots, y_m) \geq H(x_1, \ldots, x_n | y_1, \ldots, y_m)$, entropy increases with more conditioned variables
2. $H(x_1, \ldots, x_n | y_1, \ldots, y_m, z_1, \ldots, z_\ell) \leq H(x_1, \ldots, x_n | y_1, \ldots, y_m)$, entropy decreases with more conditioning variables
3. $H(x_1, \ldots, x_n, z_1, \ldots, z_\ell | y_1, \ldots, y_m) =$
   $H(x_1, \ldots, x_n | y_1, \ldots, y_m, z_1, \ldots, z_\ell) + H(z_1, \ldots, z_\ell | y_1, \ldots, y_m)$

Necessary condition for perfect secrecy

Theorem

A necessary condition for perfect secrecy and decodability is that

$$H(k) \geq H(u)$$

Proof.

Assume perfect secrecy holds, that is u is independent of x. Then,

$$\begin{aligned}
H(u) &= H(u|x) && \text{by independence of } u, x \\
&\leq H(u,k|x) && \text{by chain rule 1} \\
&= H(u|x,k) + H(k|x) && \text{by chain rule 3} \\
&= H(k|x) && \text{by perfect decodability} \\
&\leq H(k) && \text{by chain rule 2}
\end{aligned}$$

Necessary condition for perfect secrecy (cont.)

Corollary

In a system with perfect secrecy for all message distributions p_u we have

$$\log_2 |\mathcal{K}| \geq H(k) \geq \log_2 |\mathcal{M}|$$

Proof.

$H(k) \leq \log_2 |\mathcal{K}|$ is the upper bound for entropy.
From the previous theorem $H(k) \geq H(u)$ must hold for any p_u.
In particular, for uniform $u \sim \mathcal{U}(\mathcal{M})$, where $H(u) = \log_2 |\mathcal{M}|$. □

Corollary

In a system with $\mathcal{M} = \mathcal{A}^{\ell_u}$, $\mathcal{K} = \mathcal{A}^{\ell_k}$, and perfect secrecy, it is $\ell_k \geq \ell_u$

So, in order to have perfect secrecy, the key must be "at least as long as" the message.

Why "one-time"?

We may wonder if, in case several messages $u_1, u_2, \ldots$ need to be encrypted, the same key k can be reused without sacrificing perfect secrecy, that is

$$x_1 = E_k(u_1) \quad , \quad x_2 = E_k(u_2) \quad , \quad x_3 = E_k(u_3) \quad , \quad \cdots$$

Alas! This is not possible. In fact, observe that the above problem can be viewed as the encryption of a large plaintext message $u = (u_1, u_2, \ldots)$ into a large ciphertext $x = (x_1, x_2, \ldots)$ with the same key k.
So, the entropy of u increases with each u_i, while that of k remains constant, eventually violating the necessary condition for perfect secrecy

Example

In fact, it turns out that by reusing k, u is no longer statistically independent from x. For instance if $u_1 = u_2$, it must also be $x_1 = x_2$

Repeated use of the same key can only offer computational secrecy

More properties of the Kullback-Leibler divergence

1. (relation with entropy) If x, y are discrete and $y \sim \mathcal{U}(\mathcal{A}_x)$, $\mathrm{D}\left(p_x \| p_y\right) = H(y) - H(x)$.
   Proof:

$$\mathrm{D}\left(p_x \| p_y\right) = \mathrm{E}\left[\log_2 \frac{p_x(x)}{p_y(x)}\right] = \mathrm{E}\left[\log_2 p_x(x)\right] - \mathrm{E}\left[\log_2 p_y(x)\right] = -H(x) + \log_2 |\mathcal{A}_x|$$

2. (relation with mutual information) Let x, y have joint pmd p_{xy} and let x', y' be independent rvs with $p_{x'} = p_x$ and $p_{y'} = p_y$. Then,

$$\begin{aligned} \mathrm{D}\left(p_{xy} \| p_{x'y'}\right) &= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_{x'y'}(x,y)}\right] = \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_{x'}(x) p_{y'}(y)}\right] \\ &= \mathrm{E}\left[\log_2 \frac{p_{xy}(x,y)}{p_x(x) p_y(y)}\right] = I(x, y) \quad \text{(aka } \mathrm{D}\left(p_{xy} \| p_x p_y\right)\text{)} \end{aligned}$$

Measuring unconditional (not perfect) secrecy

For a non perfect secrecy system M

$$
\begin{aligned}
d(M, M^\star) &= \max_{a\in\mathcal{M}} d_{\mathsf{V}}(p_{\tilde{u}x|u=a}, p_{\tilde{u}^\star x^\star|u^\star=a}) \\
&\leq \max_{a\in\mathcal{M}} d_{\mathsf{V}}(p_{\tilde{u}x|u=a}, p_{\tilde{u}^\star x|u^\star=a}) + d_{\mathsf{V}}(p_{\tilde{u}^\star x|u=a}, p_{\tilde{u}^\star x^\star|u^\star=a}) \\
&\leq \max_{a\in\mathcal{M}} \mathrm{P}\left[\tilde{u} \neq u | u = a\right] + d_{\mathsf{V}}(p_{ux}, p_u p_x)
\end{aligned}
$$

Then, by Pinsker inequality

$$
\begin{aligned}
&\leq \max_{a\in\mathcal{M}} \mathrm{P}\left[\tilde{u} \neq u | u = a\right] + \frac{1}{2}\sqrt{\mathrm{D}\left(p_{ux} \| p_u p_x\right)} \\
&= \max_{a\in\mathcal{M}} \mathrm{P}\left[\tilde{u} \neq u | u = a\right] + \frac{1}{2}\sqrt{I(u, x)}
\end{aligned}
$$

If in a system M, we have $\mathrm{P}\left[\tilde{u} \neq u | u = a\right] \leq \varepsilon'$ and $I(u, x) \leq \varepsilon''$, then it is ε-unconditionally secure with $\varepsilon = \varepsilon' + \frac{1}{2}\sqrt{\varepsilon''}$

Classificaton of attacks against encryption

The attacks carried out against an encryption method reusing the same key for many instances are classified according to:

known ciphertext attacks (KCA) after observing N ciphertexts $x_1, \ldots, x_N$ the attacker aims to find u_N, or the key k

known plaintext attacks (KPA) after observing $N-1$ ciphertexts-plaintext pairs $(u_1, x_1), \ldots, (u_{N-1}, x_{N-1})$ and the ciphertext x_N the attacker aims to find the plaintext u_N, or the key k

chosen plaintext attacks (CPA) the attacker is allowed to access the encoder E_k; he can choose $N-1$ plaintext values $a_1, \ldots, a_{N-1} \in \mathcal{M}$ and learn the corresponding ciphertext values $b_1, \ldots, b_{N-1} \in \mathcal{X}$, with $b_i = E_k(a_i)$. Then he aims to find the plaintext u_N, or the key k from the observation of x_N

chosen ciphertext attacks (CCA) the attacker is allowed to temporarily access the decoder D_k; he can choose $N-1$ ciphertext values $b_1, \ldots, b_{N-1} \in \mathcal{X}$ and learn the corresponding plaintexts $a_1, \ldots, a_{N-1} \in \mathcal{M}$. Then he aims to find the plaintext u_N, or the key k from the observation of x_N

Classificaton of attacks against encryption

Ordering of attacks

In increasing order of strength (or information available to the attacker) we have

$$\text{KCA} < \text{KPA} < \text{CPA} < \text{KCA}$$

Which of the above attack classes can break a "one-time pad" reusing the same key k?

Summary

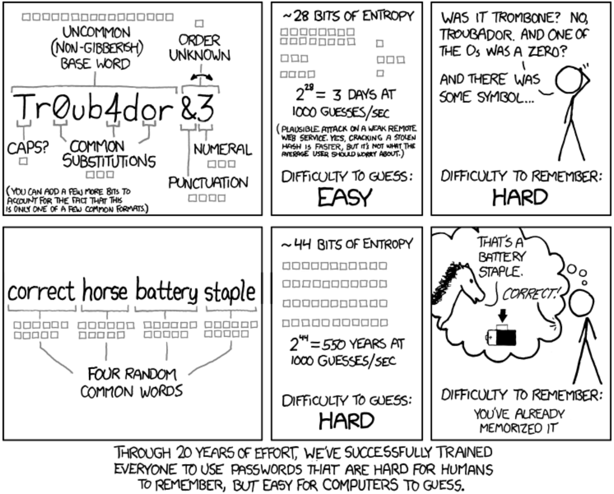
In this lecture we have:

- reviewed basic notions of Information Theory:
  - entropy of a rv
  - joint and conditional entropies
  - mutual information
- stated a necessary condition for perfect secrecy
- introduced unconditional secrecy measures
- classified attacks according to the information available to the attackers

Assignment

- class notes
- textbook, §3.4–§3.6

End of lecture



this comic reproduced from xkcd URL: `xkcd.com/936`