292 - Fall 2021
Quantitative Information Flow and Side Channels

Instructor: Tevfik Bultan

Lecture 4

Slides for this lecture are based on the following papers:

Geoffrey Smith. On the Foundations of Quantitative Information Flow. FOSSACS 2009: 288-302

Geoffrey Smith. Quantifying Information Flow Using Min-Entropy. QEST 2011: 159-167

Vulnerability with respect to information leakage

- In analyzing vulnerability of a program with respect to information leakage, we may not be solely interested in the average behavior
- In fact, we may be more interested in what happens in the worst case
- Is there a way to analyze the program to look at the worst case scenarios?

Other definitions of entropy

- Shannon entropy computes an expected value, which is a weighted average over all possibilities
- This may not be suitable if the goal is to assess vulnerability of a software system
- Rather than evaluating how much information leaks on average, we may want to evaluate how much information leaks in the worst case
- There are different entropy definitions which may be more suitable if the goal is to assess the vulnerability of a software system

Guessing entropy

- Guessing entropy G(S) is defined as the expected number of guesses required to guess S optimally
- Optimal strategy is to guess the values of S in nonincreasing order of probability

If we assume:

$$p_1 \geq p_2 \geq \ldots \geq p_n$$

then

$$G(S) = \sum_{i=1}^{n} i p_i$$

Guessing entropy vs. Shannon entropy

Shannon entropy H(S) provides a lower bound for guessing entropy G(S) (expected number of guesses required to guess S optimally)

$$G(S) \geq 2^{H(S)-2} + 1$$

assuming that H(S) is greater than or equal to 2.

Conditional Guessing entropy

Conditional guessing entropy G(S|O) is the expected number of optimal guesses required to guess S when the value of O is already known

$$G(S|O) = \sum_{o \in \mathcal{O}} P[O = o] G(S|O = o)$$

Guessing entropy vs. remaining uncertainty

Conditional entropy H(S|O) provides a lower bound for conditional guessing entropy G(S|O)

$$G(S|O) \geq 2^{H(S|O)-2} + 1$$

assuming that H(S|O) is greater than or equal to 2.

Guessing entropy

- Guessing entropy gives the expected value on the number of guesses
- Instead of the expected value of the number of guesses, we may worry about adversary guessing the value in just one try

Let P_e denote the probability that an adversary will fail to guess the value of S correctly in one try, given the value of O

- Shannon entropy can be used to give a lower bound for this value (P_e) using Fano's inequality

Fano's inequality

Let P_e denote the probability that an adversary will fail to guess the value of S correctly in one try, given the value of O.

Then, we have

$$P_e \geq (H(S|O) - 1)/\log_2(|\mathcal{S}| - 1)$$

UCSB

Lower bounds with Shannon entropy

Lower bounds provided by the Shannon entropy for $G(S|O)$ or P_e may not be very tight

This limits the usefulness of these lower bounds

Renyi entropy

Renyi-entropy

$$H_\alpha(X) = (1/(1-\alpha)) \log_2(\textstyle\sum_{x\in\mathcal{X}} P[X=x]^\alpha)$$

Renyi entropy is a family of entropy measures defined based on the parameter (order) α where $\alpha \geq 0$ and $\alpha \neq 1$

Each value of α defines a different entropy measure

UCSB

Renyi entropy, max-entropy, and Shannon entropy

Renyi-entropy

$$H_\alpha(X) = (1/(1-\alpha)) \log_2(\sum_{x \in \mathcal{X}} P[X=x]^\alpha)$$

Case $\alpha = 0$ is called max-entropy

$$H_0(X) = \log_2 |\{x \in \mathcal{X} : P[X=x] > 0\}|$$

Case $\alpha = 1$ corresponds to Shannon entropy

$$\lim_{\alpha \to 1} H_\alpha(X) = \sum_{x \in \mathcal{X}} P[X=x] \log_2(1/P[X=x])$$

Renyi entropy and min-entropy

Renyi-entropy

$$H_\alpha(X) = (1/(1-\alpha)) \log_2(\sum_{x\in\mathcal{X}} P[X=x]^\alpha)$$

Case $\alpha = \infty$ is called min-entropy

$$H_\infty(X) = \log_2(1/\max_{x\in\mathcal{X}} P[X=x])$$

UCSB

Renyi-entropy

Min-entropy is an instance of Renyi-entropy

$$H_\alpha(X) = (1/(1-\alpha)) \log_2 (\sum_{x \in \mathcal{X}} P[X = x]^\alpha)$$

where $\alpha = \infty$

So, min-entropy is also called Renyi min-entropy

If the distribution is uniform, then min-entropy is equal to the Shannon entropy

Renyi entropy

For all values of α, uniform distribution has the same Renyi entropy

I.e., if $P[X = i] = 1/n$ for $i = 1, \ldots, n$,

then,

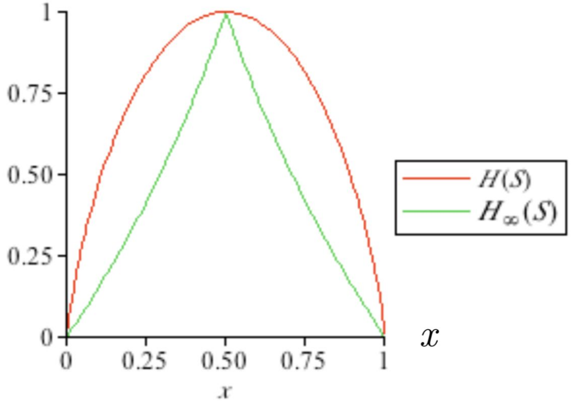
for all α, $H_\alpha(X) = \log_2 n$

α

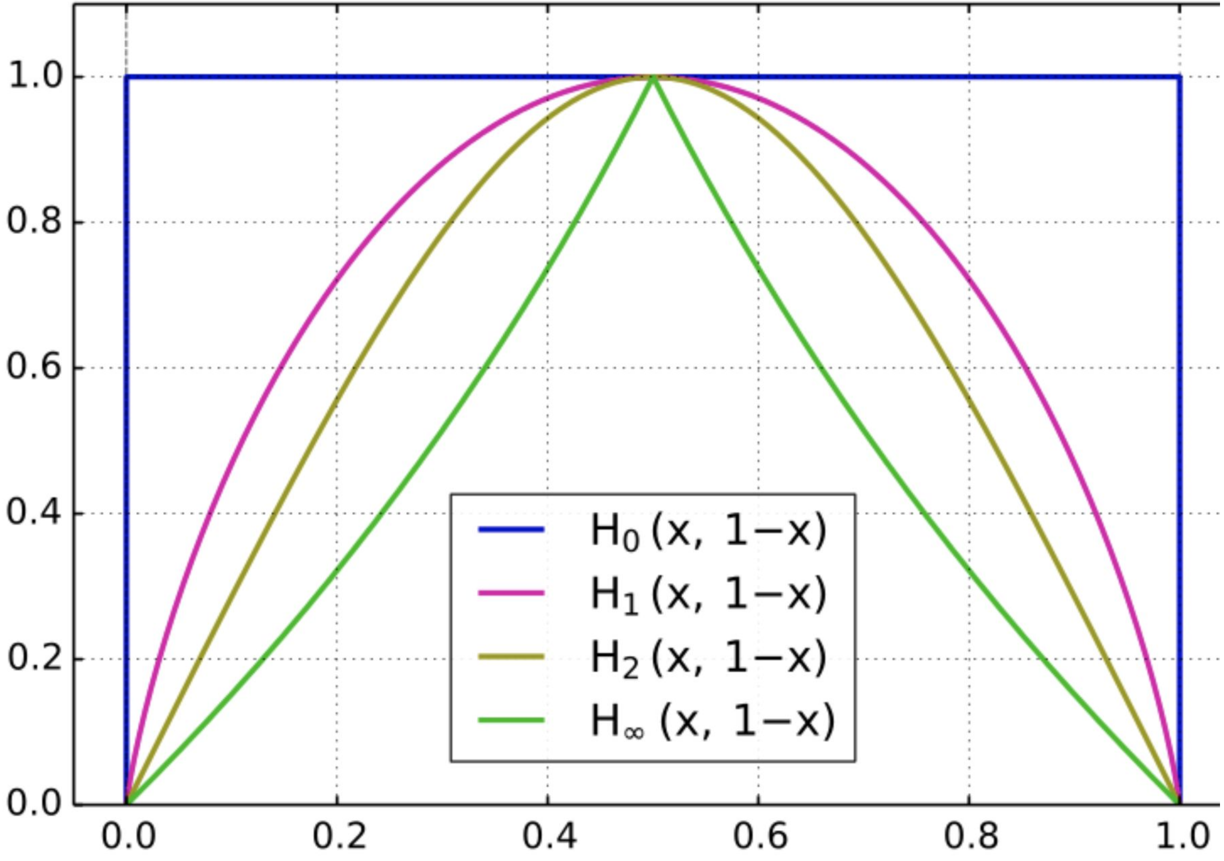
Shannon entropy vs. min-entropy

$$S = \{a, b\}$$

$$p(a) = x \quad p(b) = 1 - x$$



UCSB



Rényi entropy of a random variable with two possible outcomes against p_1, where $P = (p_1, 1 - p_1)$. Shown are H_0, H_1, H_2 and H_∞,

“vulnerability” and min-entropy

Let “vulnerability” of S be V(S), defined as

$$V(S) = \max_{s \in \mathcal{S}} P[S = s]$$

Vulnerability V(S) is the worst-case probability that an adversary could guess the value of the secret correctly in one try.

Then, min-entropy $H_\infty(S)$ is defined as

$$H_\infty(S) = \log_2(1/V(S))$$

UCSB

Conditional vulnerability

Conditional vulnerability V(S|O) is defined as:

$$V(S|O) = \sum_{o \in \mathcal{O}} P[O = o] V(S|O = o)$$

I.e., the expected value of the vulnerability, where

$$V(S|O = o) = \max_{s \in \mathcal{S}} P[S = s|O = o]$$

then, using Bayes' theorem,

$$V(S|O) = \sum_{o \in \mathcal{O}} \max_{s \in \mathcal{S}} (P[O = o|S = s] P[S = s])$$

UCSB

Conditional min-entropy

Conditional min-entropy $H_\infty(S|O)$ is defined as:

$$H_\infty(S|O) = \log_2(1/V(S|O))$$

So, now we can use the following alternative definitions

initial uncertainty: $H_\infty(S)$

remaining uncertainty: $H_\infty(S|O)$

Information leaked (min-mutual information):

$$I_\infty(S;O) = H_\infty(S) - H_\infty(S|O)$$

and, we also have:

$$V(S|O) = 2^{-H_\infty(S|O)}$$

UCSB

Deterministic programs

For deterministic programs we have

$$V(S|O) = \sum_{o \in \mathcal{O}} \max_{s \in \mathcal{S}} P[O = o|S = s][S = s]$$

Since the program is deterministic, S is partitioned to $|\mathcal{O}|$ equivalence classes by the program:

$$\mathcal{S}_o = \{s \in \mathcal{S} | \mathcal{P}[\mathcal{O} = o | \mathcal{S} = s] = 1\}$$

then

$$V(S|O) = \sum_{o \in \mathcal{O}} \max_{s \in \mathcal{S}_o} [S = s]$$

Deterministic programs and uniform distribution

For deterministic programs where the secret is uniformly distributed, we have

$$V(S) = 1/|\mathcal{S}| \text{ and } \mathcal{V}(\mathcal{S}|\mathcal{O}) = |\mathcal{O}|/|\mathcal{S}|$$

then the information leakage can be computed as:

$$I_\infty(S;O) = H_\infty(S) - H_\infty(S|O) = \log_2 |\mathcal{S}| - \log_s(|\mathcal{S}|/|\mathcal{O}|) = \log_2 |\mathcal{O}|$$

Comparing Shannon entropy and min-entropy

Assume S is a 8k-bit integer value, uniformly distributed

Program 1:

```
f(S) { if (S % 8 == 0) print S; else print 1; }
```

Program 2:

```
f(S) { print S & C }
```

where C is a binary constant and its least significant k+1 bits are one, rest are 0

Shannon entropy for programs 1 and 2

Since the input is a uniformly distributed 8k-bit integer value, for both programs 1 and 2 we have:

$$H(S) = 8k$$

Since the programs 1 and 2 are deterministic, we also have:

$$H(O|S) = 0$$

which implies that

$$I(S;O) = H(O) \text{ and } H(S|O) = H(S) - H(O)$$

Shannon entropy for program 1

We can compute H(O) for program 1 by noting that:

$P[O=1] = \frac{7}{8}$

and

$P[O=8n] = 1/2^{8k}$ for each n where $1 \leq n < 2^{8k-3}$

Then, $H(O) = \frac{7}{8} (\log_2(8/7)) + 2^{8k-3}(1/2^{8k})\log_2(1/2^{8k}) \approx k + 0.169$

which means $I(S;O) = H(O) = k + 0.169$

and $H(S|O) = H(S) - H(O) = 8k - (k + 0.169) = 7k - 0.169$

UCSB

Shannon entropy for program 2

We can compute $H(O)$ for program 2 by noting that $k+1$ bits of S is copied to O, so

$H(O) = k + 1$

which means $I(S;O) = k + 1$

and $H(S|O) = H(S) - H(O) = 8k - (k + 1) = 7k - 1$

Shannon entropy for programs 1 and 2

According to Shannon entropy, amount of information leaked and remaining uncertainty for programs 1 and 2 are:

Program 1: leakage: $I(S;O) = k + 0.169$ $H(S|O) = 7k - 0.169$

Program 2: leakage: $I(S;O) = k + 1$ $H(S|O) = 7k - 1$

Shannon entropy for programs 1 and 2

So, Program 2 leaks more information according to Shannon entropy.

Note that, program 1 leaks the full secret ⅛ of the time, whereas for program 2, 7k-1 bits of information remains uncertain for all cases

So, in the worst case, program 1 leaks much more information than program 2, but since Shannon entropy focuses on average case, it concludes that program 2 leaks more information

Min entropy for programs 1 and 2

Since the input is a uniformly distributed 8k-bit integer value, for both programs 1 and 2 we have:

$$H_\infty(S) = 8k$$

Min entropy for programs 1 and 2

Since secret is uniformly distributed and the programs are deterministic, for both programs 1 and 2, the information leakage is

$$\log_2 |\mathcal{O}|$$

For program 1:

$$\log_2 |\mathcal{O}| = 8k - 3$$

For program 2:

$$\log_2 |\mathcal{O}| = k + 1$$

UCSB

Min-entropy for programs 1 and 2

According to min-entropy, amount of information leaked and remaining uncertainty for programs 1 and 2 are:

Program 1: leakage: $I_\infty(S;O) = 8k - 3$ $H_\infty(S|O) = 3$

Program 2: leakage: $I_\infty(S;O) = k + 1$ $H_\infty(S|O) = 7k - 1$

Min-entropy for programs 1 and 2

Since min-entropy focuses on the worst-case probability that an adversary could guess the value of the secret correctly in one try, the leakage computed for program 1 increases significantly

According the min-entropy, program 1 leaks much more information than program 2 for large values of k.