Preventing Side-Channel Leaks in Web Traffic: A Formal Approach

Goran Doychev

IMDEA Software Institute

joint work with

Michael Backes and Boris Köpf

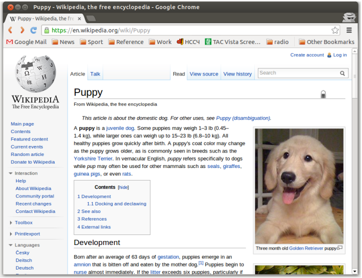
20th Network & Distributed System Security Symposium

San Diego, CA

February 25, 2013

Leaks in Web Traffic

Leaks in Web Traffic



Puppy

From Wikipedia, the free encyclopedia

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

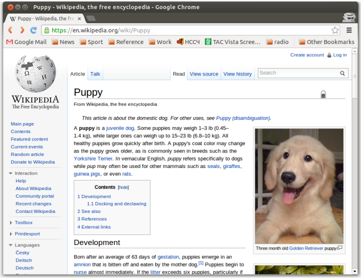
Contents [hide]

Three month old Golden Retriever puppy

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Leaks in Web Traffic



Puppy

From Wikipedia, the free encyclopedia

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

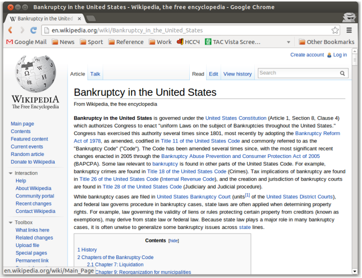
Three month old Golden Retriever puppy

Contents [hide]

1 Development
1.1 Docking and declawing
2 See also
3 References
4 External links

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if



Bankruptcy in the United States

From Wikipedia, the free encyclopedia

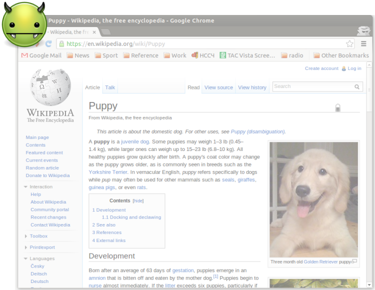
Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

While bankruptcy cases are filed in United States Bankruptcy Court (units[1] of the United States District Courts), and federal law governs procedure in bankruptcy cases, state laws are often applied when determining property rights. For example, law governing the validity of liens or rules protecting certain property from creditors (known as exemptions), may derive from state law or federal law. Because state law plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

Leaks in Web Traffic



Puppy

From Wikipedia, the free encyclopedia

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

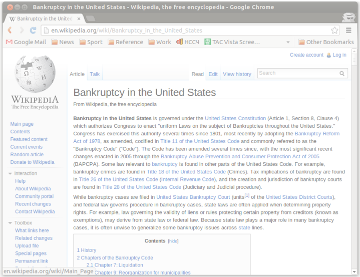
Contents [hide]

1 Development
1.1 Docking and declawing
2 See also
3 References
4 External links

Three month old Golden Retriever puppy

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if



Bankruptcy in the United States

From Wikipedia, the free encyclopedia

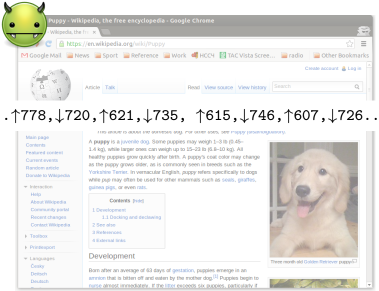
Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

While bankruptcy cases are filed in United States Bankruptcy Court (units[1] of the United States District Courts), and federal law governs procedure in bankruptcy cases, state laws are often applied when determining property rights. For example, law governing the validity of liens or rules protecting certain property from creditors (known as exemptions), may derive from state law or federal law. Because state law plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

Leaks in Web Traffic



Puppy - Wikipedia, the free encyclopedia - Google Chrome

- Wikipedia, the fre ×

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

Google Mail | News | Sport | Reference | Work | HCCЧ | TAC Vista Scree... | radio | Other Bookmarks

Create account | Log in

Article | Talk | Read | View source | View history | Search

...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

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

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages
Česky
Deitsch
Deutsch

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

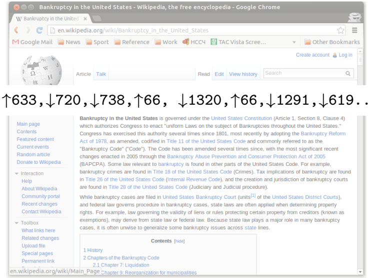
Contents [hide]

1 Development
1.1 Docking and declawing
2 See also
3 References
4 External links

Three month old Golden Retriever puppy

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if



Bankruptcy in the United States - Wikipedia, the free encyclopedia - Google Chrome

Bankruptcy in the United ×

en.wikipedia.org/wiki/Bankruptcy_in_the_United_States

Google Mail | News | Sport | Reference | Work | HCCЧ | TAC Vista Scree... | Other Bookmarks

Create account | Log in

Article | Talk | Read | Edit | View history | Search

...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

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

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox
What links here
Related changes
Upload file
Special pages
Permanent link

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

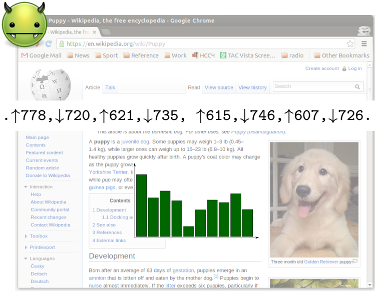
While bankruptcy cases are filed in United States Bankruptcy Court (units[1] of the United States District Courts), and federal law governs procedure in bankruptcy cases, state laws are often applied when determining property rights. For example, law governing the validity of liens or rules protecting certain property from creditors (known as exemptions), may derive from state law or federal law. Because state law plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

en.wikipedia.org/wiki/Main_Page

Leaks in Web Traffic



...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

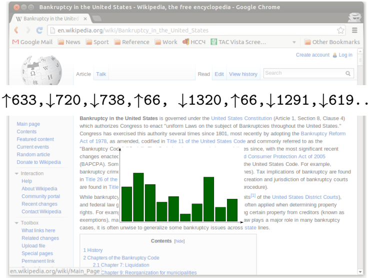
A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows Yorkshire Terrier. I while *pup* may ofte guinea pigs, or eve

Contents
1 Development
1.1 Docking a
2 See also
3 References
4 External links

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Three month old Golden Retriever puppy



...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

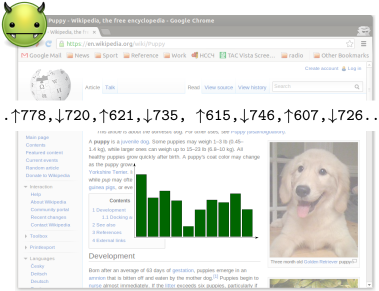
Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Cod es since, with the most significant recent changes enacted d Consumer Protection Act of 2005 (BAPCPA). Som the United States Code. For example, bankruptcy crime nes). Tax implications of bankruptcy are found in Title 26 of the creation and jurisdiction of bankruptcy courts are found in Title procedure).

While bankruptcy nits[1] of the United States District Courts), and federal law g often applied when determining property rights. For examp g certain property from creditors (known as exemptions), ma aw plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]
1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

- an attack: compare distributions of packet sizes (Liberatore et al.'06)

Leaks in Web Traffic



Puppy - Wikipedia, the free encyclopedia - Google Chrome

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

...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows Yorkshire Terrier. I while *pup* may ofte guinea pigs, or eve

Contents

1 Development

1.1 Docking a

2 See also

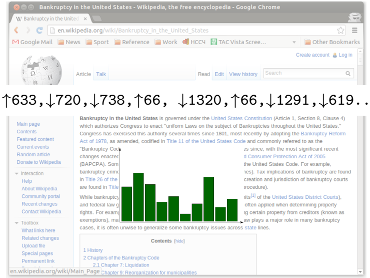
3 References

4 External links

Three month old Golden Retriever puppy

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if



Bankruptcy in the United States - Wikipedia, the free encyclopedia - Google Chrome

en.wikipedia.org/wiki/Bankruptcy_in_the_United_States

...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Cod es since, with the most significant recent changes enacted d Consumer Protection Act of 2005 (BAPCPA). Som the United States Code. For example, bankruptcy crime nes). Tax implications of bankruptcy are found in Title 26 of the creation and jurisdiction of bankruptcy courts are found in Title procedure).

While bankruptcy nits[1] of the United States District Courts), and federal law g often applied when determining property rights. For examp ng certain property from creditors (known as exemptions), ma aw plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History

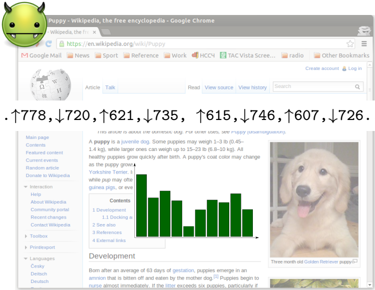
2 Chapters of the Bankruptcy Code

2.1 Chapter 7: Liquidation

Chapter 9: Reorganization for municipalities

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)

Leaks in Web Traffic



Puppy - Wikipedia, the free encyclopedia - Google Chrome

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

...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows Yorkshire Terrier. I while *pup* may ofte guinea pigs, or eve

Contents

1 Development

1.1 Docking a

2 See also

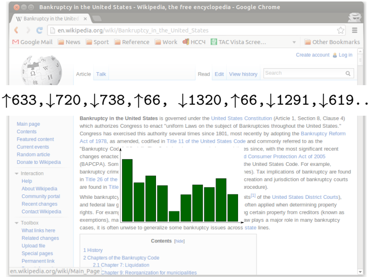
3 References

4 External links

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Three month old Golden Retriever puppy



Bankruptcy in the United States - Wikipedia, the free encyclopedia - Google Chrome

en.wikipedia.org/wiki/Bankruptcy_in_the_United_States

...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Cod es since, with the most significant recent changes enacted d Consumer Protection Act of 2005 (BAPCPA). Som the United States Code. For example, bankruptcy crime nes). Tax implications of bankruptcy are found in Title 26 of the creation and jurisdiction of bankruptcy courts are found in Title procedure).

While bankruptcy nits[1] of the United States District Courts), and federal law g often applied when determining property rights. For examp ng certain property from creditors (known as exemptions), ma aw plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History

2 Chapters of the Bankruptcy Code

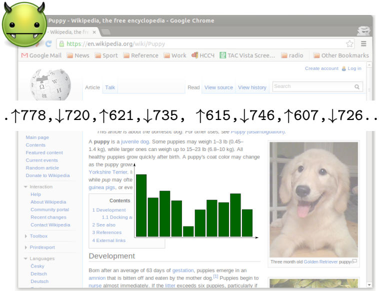
2.1 Chapter 7: Liquidation

Chapter 9: Reorganization for municipalities

en.wikipedia.org/wiki/Main_Page

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)

Leaks in Web Traffic



Puppy - Wikipedia, the free encyclopedia - Google Chrome

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

...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

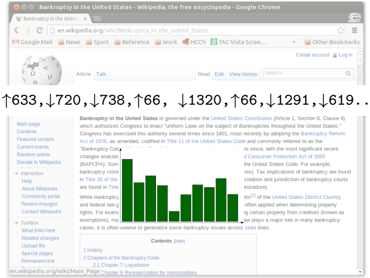
A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows Yorkshire Terrier. I while *pup* may ofte guinea pigs, or eve

Contents
1 Development
1.1 Docking a
2 See also
3 References
4 External links

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Three month old Golden Retriever puppy



Bankruptcy in the United States - Wikipedia, the free encyclopedia - Google Chrome

en.wikipedia.org/wiki/Bankruptcy_in_the_United_States

...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Cod es since, with the most significant recent changes enactec d Consumer Protection Act of 2005 (BAPCPA). Som the United States Code. For example, bankruptcy crime nes). Tax implications of bankruptcy are found in Title 26 of the creation and jurisdiction of bankruptcy courts are found in Title procedure).

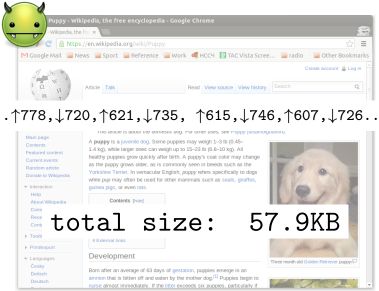
While bankruptcy nits[1] of the United States District Courts), and federal law g often applied when determining property rights. For examp g certain property from creditors (known as exemptions), ma aw plays a major role in many bankruptcy cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]
1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

en.wikipedia.org/wiki/Main_Page

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

Leaks in Web Traffic



...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

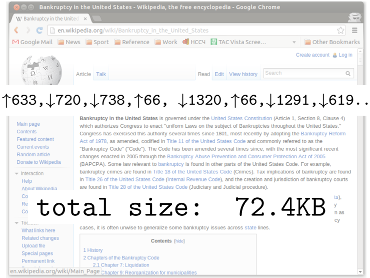
A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

Three month old Golden Retriever puppy

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

total size: 57.9KB



...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

cases, it is often unwise to generalize some bankruptcy issues across state lines.

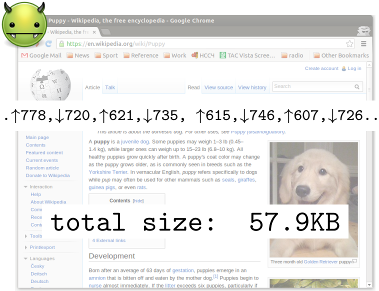
Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

total size: 72.4KB

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

Leaks in Web Traffic



...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

Contents [hide]

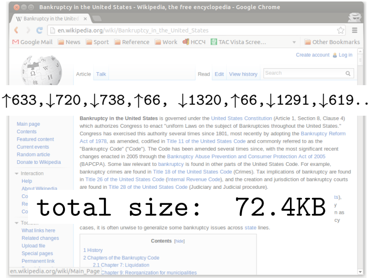
4 External links

total size: 57.9KB

Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Three month old Golden Retriever puppy



...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

total size: 72.4KB

cases, it is often unwise to generalize some bankruptcy issues across state lines.

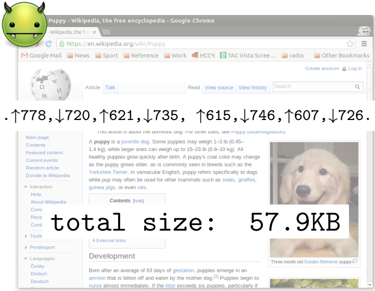
Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

How to show that a countermeasure is "good"?

Leaks in Web Traffic



This article is about the domestic dog. For other uses, see Puppy (disambiguation).

A **puppy** is a juvenile dog. Some puppies may weigh 1–3 lb (0.45–1.4 kg), while larger ones can weigh up to 15–23 lb (6.8–10 kg). All healthy puppies grow quickly after birth. A puppy's coat color may change as the puppy grows older, as is commonly seen in breeds such as the Yorkshire Terrier. In vernacular English, *puppy* refers specifically to dogs while *pup* may often be used for other mammals such as seals, giraffes, guinea pigs, or even rats.

Contents [hide]

4 External links

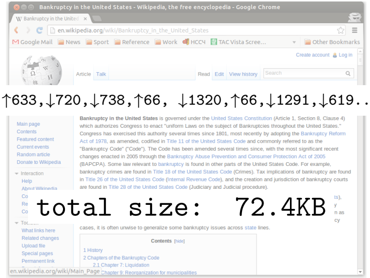
Development

Born after an average of 63 days of gestation, puppies emerge in an amnion that is bitten off and eaten by the mother dog.[1] Puppies begin to nurse almost immediately. If the litter exceeds six puppies, particularly if

Three month old Golden Retriever puppy

...↑778,↓720,↑621,↓735, ↑615,↓746,↑607,↓726...

total size: 57.9KB



Bankruptcy in the United States is governed under the United States Constitution (Article 1, Section 8, Clause 4) which authorizes Congress to enact "uniform Laws on the subject of Bankruptcies throughout the United States." Congress has exercised this authority several times since 1801, most recently by adopting the Bankruptcy Reform Act of 1978, as amended, codified in Title 11 of the United States Code and commonly referred to as the "Bankruptcy Code" ("Code"). The Code has been amended several times since, with the most significant recent changes enacted in 2005 through the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Some law relevant to bankruptcy is found in other parts of the United States Code. For example, bankruptcy crimes are found in Title 18 of the United States Code (Crimes). Tax implications of bankruptcy are found in Title 26 of the United States Code (Internal Revenue Code), and the creation and jurisdiction of bankruptcy courts are found in Title 28 of the United States Code (Judiciary and Judicial procedure).

cases, it is often unwise to generalize some bankruptcy issues across state lines.

Contents [hide]

1 History
2 Chapters of the Bankruptcy Code
2.1 Chapter 7: Liquidation
Chapter 9: Reorganization for municipalities

...↑633,↓720,↓738,↑66, ↓1320,↑66,↓1291,↓619...

total size: 72.4KB

- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

How to show that a countermeasure is "good"?

- previous work: empirically show that a particular attack does not work

Our approach

Reason *formally* about strength of countermeasures

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

↪ models provide explicit assumptions

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

↪ models provide explicit assumptions

Main contributions:

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

↪ models provide explicit assumptions

Main contributions:

- simple, yet realistic models

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

↪ models provide explicit assumptions

Main contributions:

- simple, yet realistic models
- efficient algorithms for measuring and reducing information leakage

Our approach

Reason *formally* about strength of countermeasures

1. models of web applications, web traffic, users and adversaries
2. derive security guarantees based on model

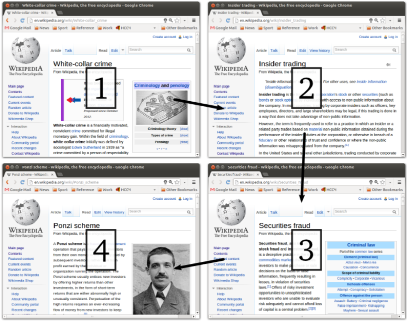
↪ models provide explicit assumptions

Main contributions:

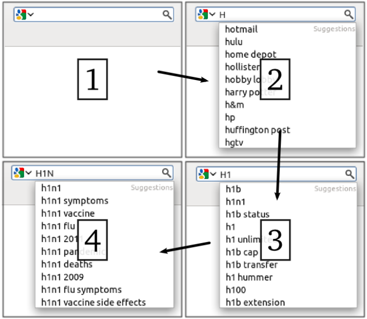
- simple, yet realistic models
- efficient algorithms for measuring and reducing information leakage
- demonstrate approach in case studies

Modeling web applications

Static website

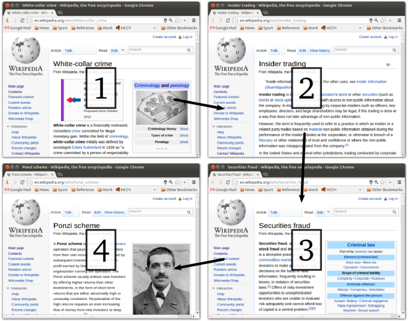


Auto-suggest input field

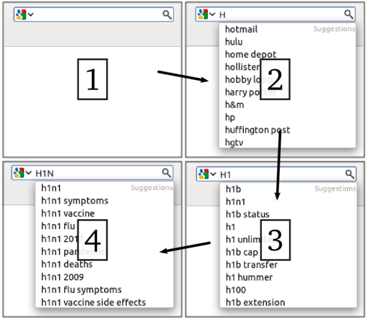


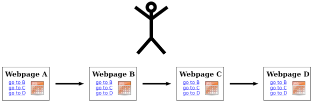
Modeling web applications

Static website



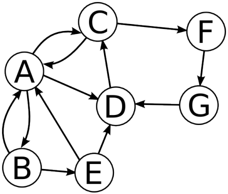
Auto-suggest input field



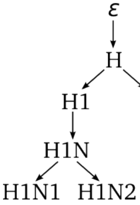


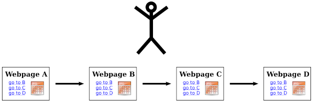
Modeling web applications

Static website

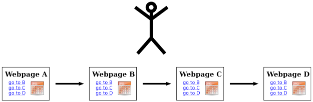


Auto-suggest input field

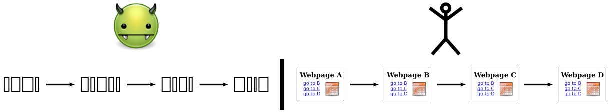




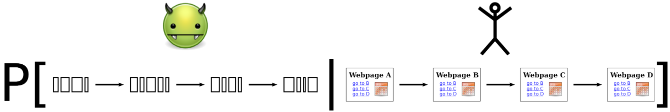
The traffic channel



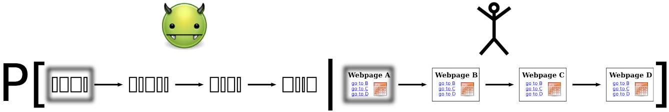
The traffic channel



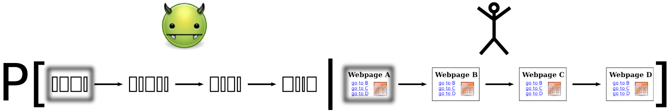
The traffic channel

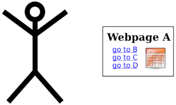


The traffic channel

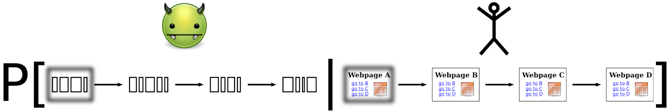


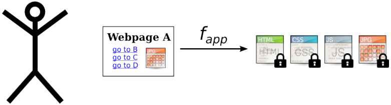
The traffic channel



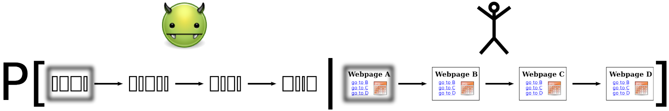


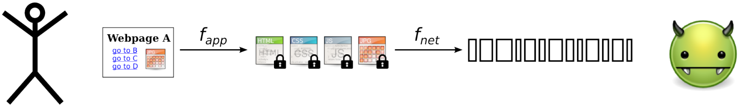
The traffic channel



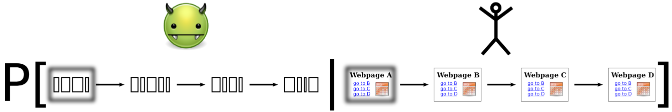


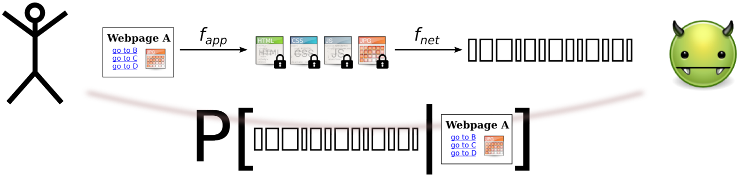
The traffic channel



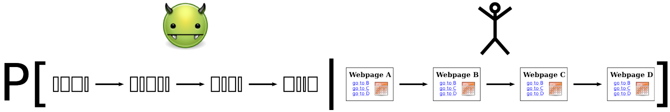


The traffic channel

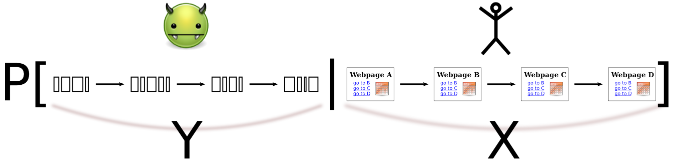




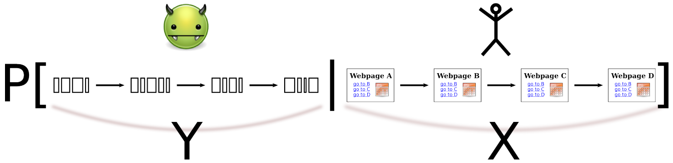
Measuring security in the system



Measuring security in the system

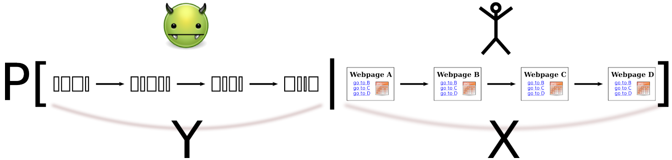


Measuring security in the system



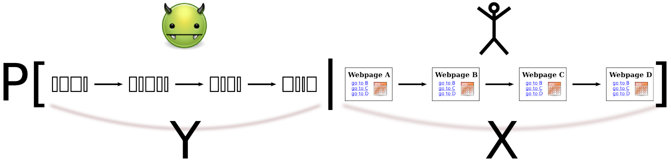
- security measure: difficulty of guessing X when Y is known

Measuring security in the system

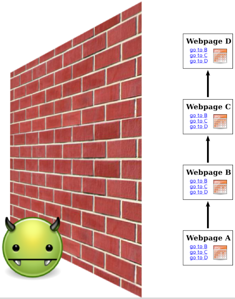


- security measure: difficulty of guessing X when Y is known
- expected $\#$ guesses: captured by entropy H (Massey'94)

Measuring security in the system

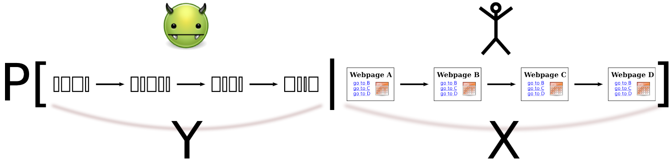


- security measure: difficulty of guessing X when Y is known
- expected # guesses: captured by entropy H (Massey'94)

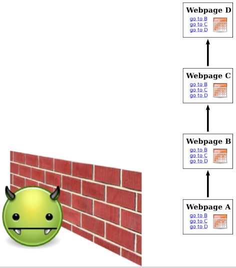


- initial uncertainty $H(X)$

Measuring security in the system

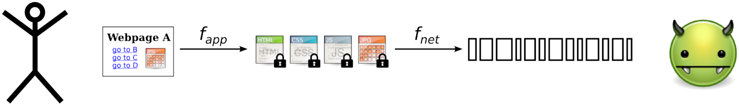


- security measure: difficulty of guessing X when Y is known
- expected # guesses: captured by entropy H (Massey'94)

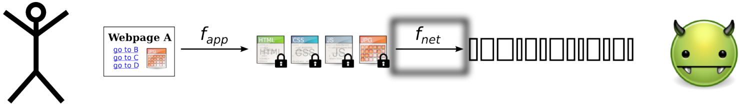


- initial uncertainty $H(X)$
- remaining uncertainty $H(X|Y)$

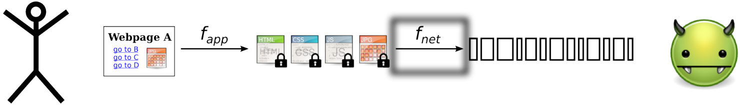
Traffic modifiers: countermeasures, network protocols



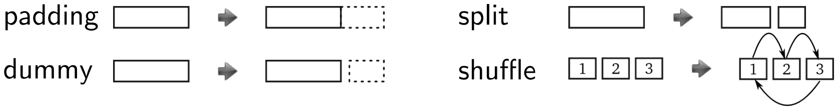
Traffic modifiers: countermeasures, network protocols



Traffic modifiers: countermeasures, network protocols



Basic traffic modifiers:



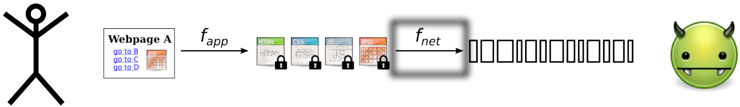
padding

dummy

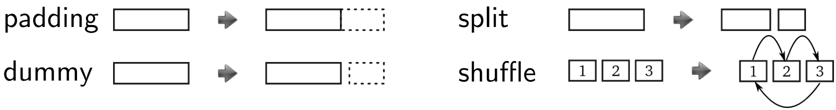
split

shuffle

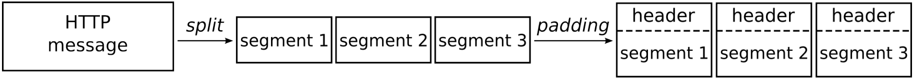
Traffic modifiers: countermeasures, network protocols



Basic traffic modifiers:

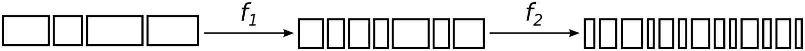


Example (Packet segmentation)



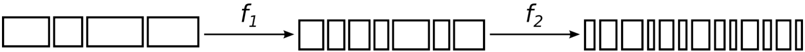
Composition theorem

Composed traffic modifier $f_2 \circ f_1$:



Composition theorem

Composed traffic modifier $f_2 \circ f_1$:

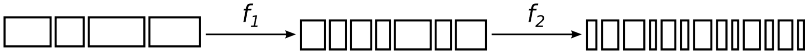


Theorem

$$H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$$

Composition theorem

Composed traffic modifier $f_2 \circ f_1$:



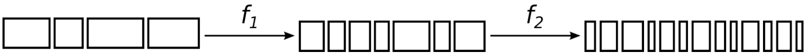
Theorem

$$H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$$

- proof relies on *data processing inequality*

Composition theorem

Composed traffic modifier $f_2 \circ f_1$:



Theorem

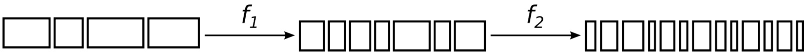
$$H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$$

- proof relies on *data processing inequality*

Consequence: relative security guarantees for free

Composition theorem

Composed traffic modifier $f_2 \circ f_1$:



Theorem

$$H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$$

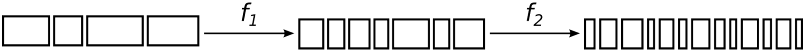
- proof relies on *data processing inequality*

Consequence: relative security guarantees for free

- countermeasure $f_2 \circ f_1$ at least as strong as f_1

Composition theorem

Composed traffic modifier $f_2 \circ f_1$:



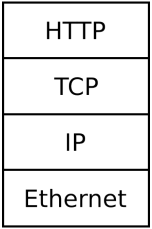
Theorem

$$H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$$

- proof relies on *data processing inequality*

Consequence: relative security guarantees for free

- countermeasure $f_2 \circ f_1$ at least as strong as f_1
- security guarantees preserved when message passes protocol stack



How to evaluate real-world websites?

How to evaluate real-world websites?

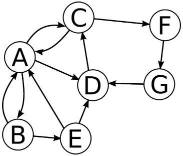
Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$

How to evaluate real-world websites?

Computing the remaining uncertainty:

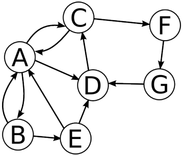
- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths

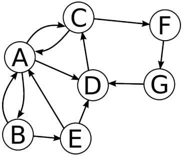


Our approach:

How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



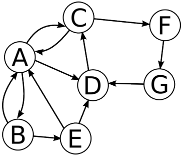
Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain

How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



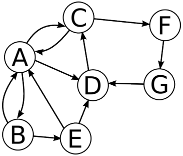
Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



Our approach:

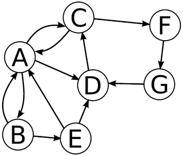
- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1]$ = stationary distribution

$\Rightarrow$ $H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$

How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1]$ = stationary distribution

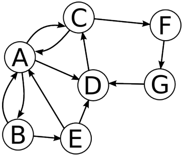
$\Rightarrow$ $H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$

Obtaining the stationary distribution: use PageRank algorithm

How to evaluate real-world websites?

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths



Our approach:

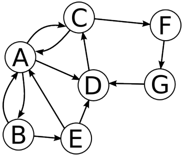
- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1]$ = stationary distribution

$\Rightarrow$ $H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$

Obtaining the stationary distribution: use PageRank algorithm

- PageRank algorithm computes the stationary distribution of X

How to evaluate real-world websites?



Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) - H(Y)$
- direct computation of $H(X)$ not feasible: have to enumerate of all paths

Our approach:

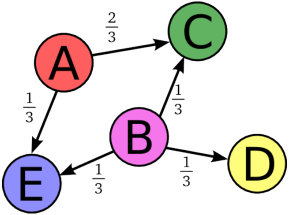
- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

$\Rightarrow$ $H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$

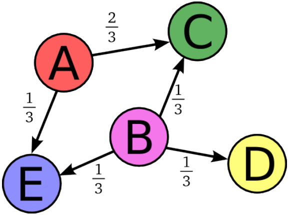
Obtaining the stationary distribution: use PageRank algorithm

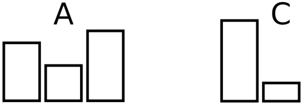
- PageRank algorithm computes the stationary distribution of X
- random surfer: follow random link or jump to random page

Path-aware countermeasures

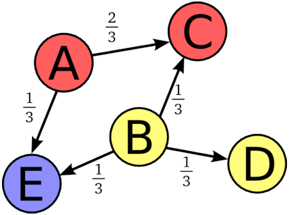


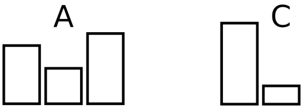
Path-aware countermeasures





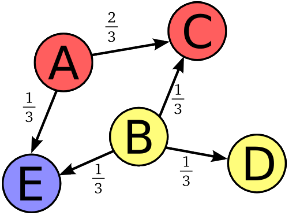
Path-aware countermeasures

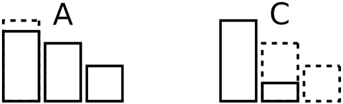




Countermeasures make vertices indistinguishable

Path-aware countermeasures

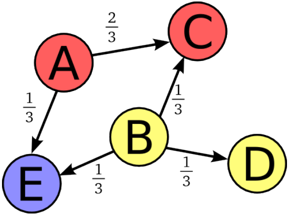


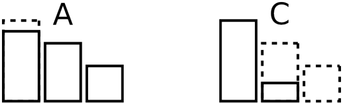


Countermeasures make vertices indistinguishable

- e.g. `c_order`: order objects by size, pad, add dummy objects

Path-aware countermeasures

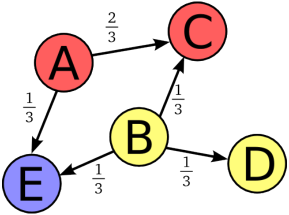


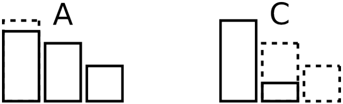


Countermeasures make vertices indistinguishable

- e.g. `c_order`: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices

Path-aware countermeasures



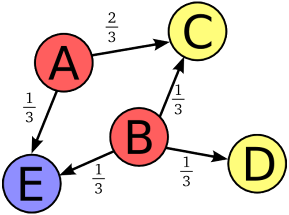


Countermeasures make vertices indistinguishable

- e.g. `c_order`: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices

Paths may not be indistinguishable

Path-aware countermeasures



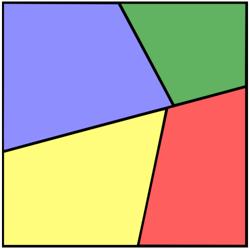
Countermeasures make vertices indistinguishable

- e.g. `c_order`: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices

Paths may not be indistinguishable

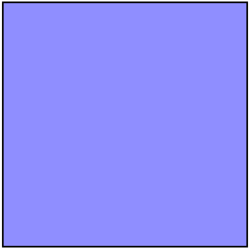
⇒ ensure partition of vertices is a *probabilistic bisimulation*

Path-aware countermeasures (2)



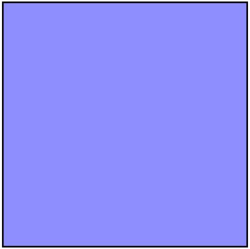
- there are many possible bisimulations

Path-aware countermeasures (2)



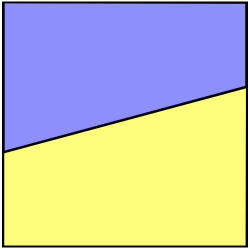
- there are many possible bisimulations

Path-aware countermeasures (2)



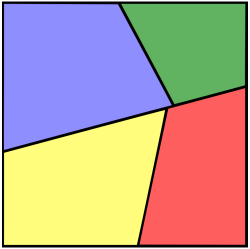
- there are many possible bisimulations
- our approach: consider random bisimulations

Path-aware countermeasures (2)



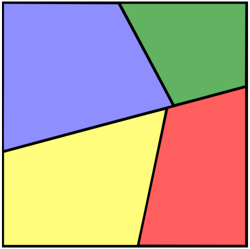
- there are many possible bisimulations
- our approach: consider random bisimulations
  1. start from random bi-partition

Path-aware countermeasures (2)



- there are many possible bisimulations
- our approach: consider random bisimulations
  1. start from random bi-partition
  2. refine it to coarsest bisimulation /* Derisavi et al.'03 */

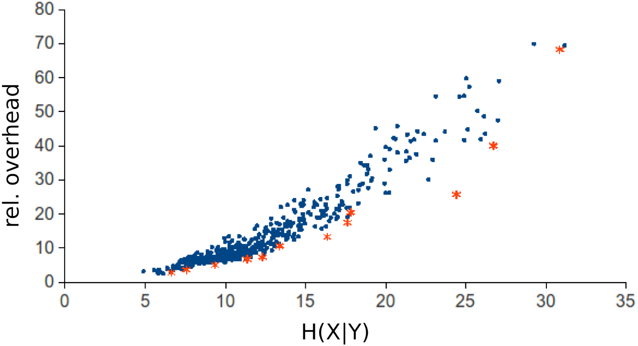
Path-aware countermeasures (2)



- there are many possible bisimulations
- our approach: consider random bisimulations
  1. start from random bi-partition
  2. refine it to coarsest bisimulation /* Derisavi et al.'03 */
  3. repeat

Case study

Trading security for overhead : 500 random bisimiulations



Case study (2)

Case study (2)

Analyzed website:

- `bar.wikipedia.org` ($\approx$ 3,500 pages)

Case study (2)

Analyzed website:

- bar.wikipedia.org ($\approx$ 3,500 pages)

Initial uncertainty:

ℓ	1	3	5	9	15	25	40
$H(X)$	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	$2^{36.5}$	$2^{59.8}$	2^{106}	2^{176}	2^{295}	2^{472}

Case study (2)

Analyzed website:

- `bar.wikipedia.org` ($\approx$ 3,500 pages)

Initial uncertainty:

ℓ	1	3	5	9	15	25	40
$H(X)$	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	$2^{36.5}$	$2^{59.8}$	2^{106}	2^{176}	2^{295}	2^{472}

No countermeasure:

- $H(X|Y) = 0$

Case study (2)

Analyzed website:

- `bar.wikipedia.org` ($\approx$ 3,500 pages)

Initial uncertainty:

ℓ	1	3	5	9	15	25	40
$H(X)$	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	$2^{36.5}$	$2^{59.8}$	2^{106}	2^{176}	2^{295}	2^{472}

No countermeasure:

- $H(X|Y) = 0$

Applying path-aware countermeasures (path length $\ell = 5$):

Case study (2)

Analyzed website:

- `bar.wikipedia.org` ($\approx$ 3,500 pages)

Initial uncertainty:

ℓ	1	3	5	9	15	25	40
$H(X)$	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	$2^{36.5}$	$2^{59.8}$	2^{106}	2^{176}	2^{295}	2^{472}

No countermeasure:

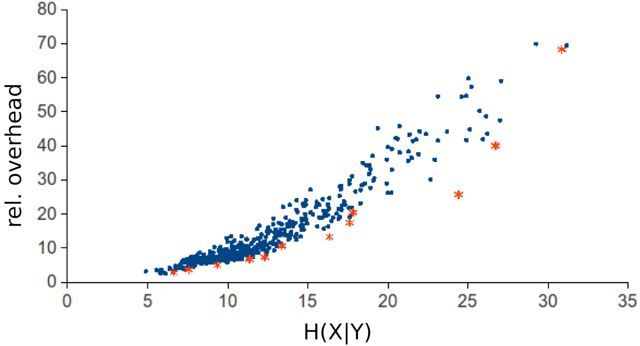
- $H(X|Y) = 0$

Applying path-aware countermeasures (path length $\ell = 5$):

- make all webpages have the same fingerprint: expected overhead 73.5 × original size

Case study (3)

Trading security for overhead: 500 random bisimiulations



Bonus material in the paper

- limits on overhead of path-aware countermeasure
- case study: auto-complete field
- using other entropy measures
- timing leaks: combining security guarantees with predictive timing mitigation (Askarov et al.'10)

Summary

Summary

- formal framework for reasoning about security of web applications

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations
- demonstrate approach in case studies

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations
- demonstrate approach in case studies