Why Privacy Matters?

Some Thoughts About Privacy And Mobile Application Security

15.6.2011

So What About Privacy?

Privacy has quickly become the new buzzword and motivation for security especially in mobile personal devices.

Why?

Some people and organizations think privacy is not a big deal

- Only criminals want to hide their intentions and actions
- He who has nothing to hide has nothing to fear
- Who in earth would care about my messages, contacts or calender entries?
  Surely I am not that important!

Naturally it isn't so. But why?

So What About Privacy?

Privacy has quickly become the new buzzword and motivation for security especially in mobile personal devices.

Why?

Some people and organizations think privacy is not a big deal

- Only criminals want to hide their intentions and actions
- He who has nothing to hide has nothing to fear
- Who in earth would care about my messages, contacts or calender entries?
  Surely I am not that important!

Naturally it isn't so. But why?

An Engineer's Viewpoint

Some practical reasons why private information should be protected especially when it is easily searchable

- Oppressive authorities can use private information wrong
- Criminals can use it for their own purposes
- Combining innocent data from multiple sources can reveal more about us than we feel comfortable with

But There Is More

Juha Räikkä: Yksityisyyden filosofia, WSOY 2007

People define their social distance from each other by choosing what to share and what not.

- Private knowledge is a social currency
- It looses its value if it becomes public
- Hence protecting privacy is protecting private property and its owner's autonomy

But There Is More

Juha Räikkä: Yksityisyyden filosofia, WSOY 2007

People define their social distance from each other by choosing what to share and what not.

- Private knowledge is a social currency
- It looses its value if it becomes public
- Hence protecting privacy is protecting private property and its owner's autonomy

But There Is More

Juha Räikkä: Yksityisyyden filosofia, WSOY 2007

People define their social distance from each other by choosing what to share and what not.

- Private knowledge is a social currency
- It looses its value if it becomes public
- Hence protecting privacy is protecting private property and its owner's autonomy

But There Is More

Juha Räikkä: Yksityisyyden filosofia, WSOY 2007

People define their social distance from each other by choosing what to share and what not.

- Private knowledge is a social currency
- It looses its value if it becomes public
- Hence protecting privacy is protecting private property and its owner's autonomy

Social Media

How come many people then share so openly in the social media?

- Privacy is a commodity that can be exchanged for other commodities: popularity, sense of belonging to a group etc.
- Different roles in different contexts are (falsely) expected to remain isolated.
- People may decide to give up some of their privacy but they will not negotiate of their right to make that decision.

If people feel their right to control their own privacy is not respected they will be extremely annoyed. No matter how harmless the leaked data is or if the disclosure was accidental or not, they will feel *violated* and *defiled*.

Social Media

How come many people then share so openly in the social media?

- Privacy is a commodity that can be exchanged for other commodities: popularity, sense of belonging to a group etc.
- Different roles in different contexts are (falsely) expected to remain isolated.
- People may decide to give up some of their privacy but they will not negotiate of their right to make that decision.

If people feel their right to control their own privacy is not respected they will be extremely annoyed. No matter how harmless the leaked data is or if the disclosure was accidental or not, they will feel *violated* and *defiled*.

Social Media

How come many people then share so openly in the social media?

- Privacy is a commodity that can be exchanged for other commodities: popularity, sense of belonging to a group etc.
- Different roles in different contexts are (falsely) expected to remain isolated.
- People may decide to give up some of their privacy but they will not negotiate of their right to make that decision.

If people feel their right to control their own privacy is not respected they will be extremely annoyed. No matter how harmless the leaked data is or if the disclosure was accidental or not, they will feel *violated* and *defiled*.

Social Media

How come many people then share so openly in the social media?

- Privacy is a commodity that can be exchanged for other commodities: popularity, sense of belonging to a group etc.
- Different roles in different contexts are (falsely) expected to remain isolated.
- People may decide to give up some of their privacy but they will not negotiate of their right to make that decision.

If people feel their right to control their own privacy is not respected they will be extremely annoyed. No matter how harmless the leaked data is or if the disclosure was accidental or not, they will feel *violated* and *defiled*.

Social Media

How come many people then share so openly in the social media?

- Privacy is a commodity that can be exchanged for other commodities: popularity, sense of belonging to a group etc.
- Different roles in different contexts are (falsely) expected to remain isolated.
- People may decide to give up some of their privacy but they will not negotiate of their right to make that decision.

If people feel their right to control their own privacy is not respected they will be extremely annoyed. No matter how harmless the leaked data is or if the disclosure was accidental or not, they will feel *violated* and *defiled*.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

In Practice This Means

When making a mobile application ensure that

- No information it stores is shared with anyone without clear user's consent. Not even other applications in the same device. The content of the information does not really count. What counts is that since it is created in the device, it belongs to the device's owner.
- Use local system's protections and cryptography if available to make sure no accidental sharing takes place.
- If consolidating data from multiple devices at user's consent, make it untraceable. Document how it is done.
- Be absolutely clear what data is being gathered and for what purpose. Do not change the rules later.

Marketing data is valuable, so be prepared to offer a compensation for those who are willing to give it. Do not try to steal it.

Why Privacy Matters?

The whole story soon at
`https://www.nixuopen.org/blog`

`juhani.makela@nixuopen.org`