Applying Privacy by Design as a Strategy to Reduce Your Attack Surface

ICTTF Cyber Threat Summit

Chuck Georgo

October 24, 2017

NOWHERE TO HIDE.ORG

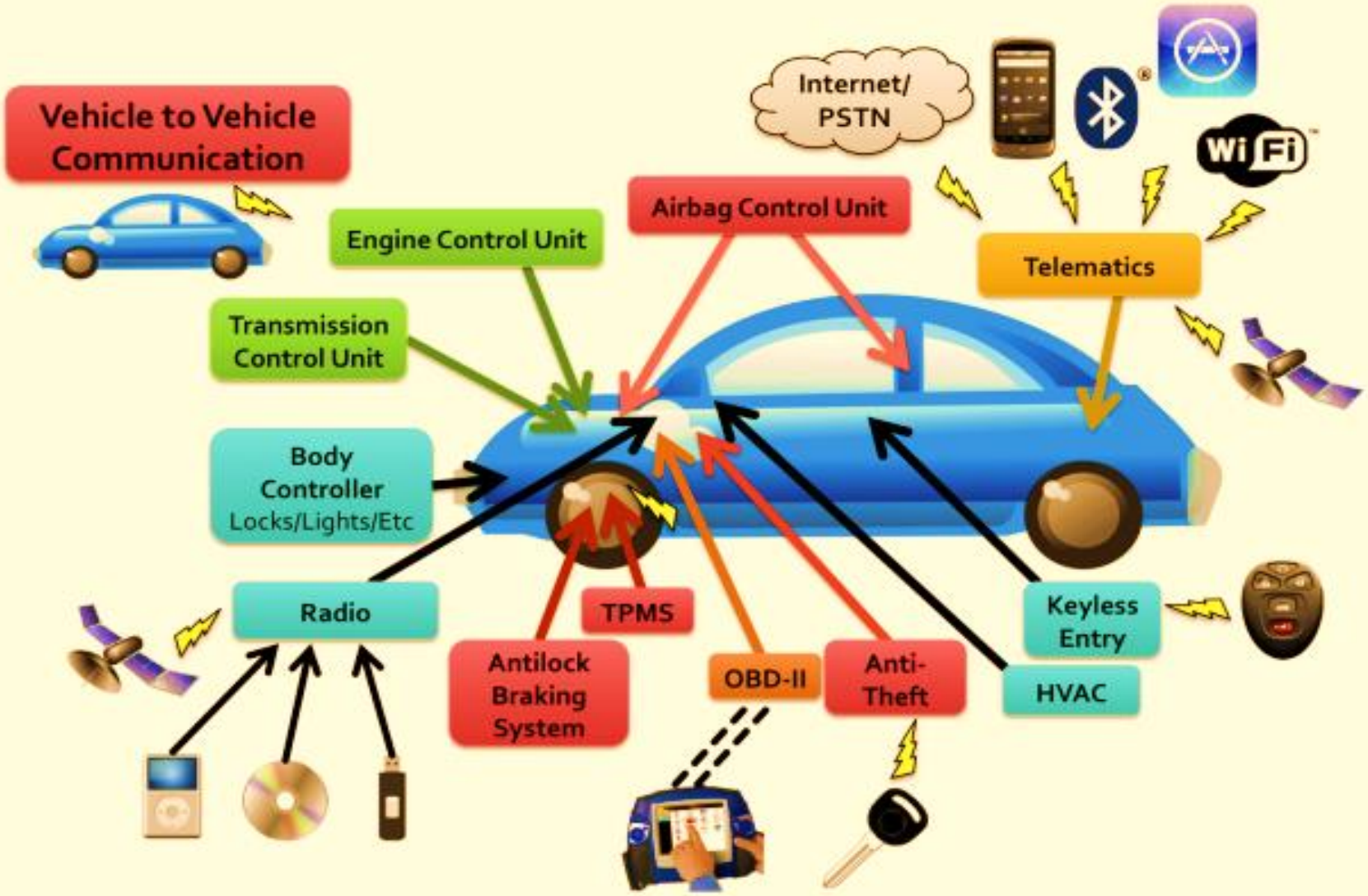

Once upon a time


Show
Me the
Cyber
Security

Hacker tools are now a commodity…

Digital islands simply do not exist…

IoT exposes more attack opportunities…



Intrusion prevention continues to be elusive…

Best practices are proving to be ineffective…

Updates and patching now a source of malware…


So, how can addressing
privacy help?

What is the attack surface here?

And, here's your typical defense


But what about the stuff inside?

This is your organization's attack surface…

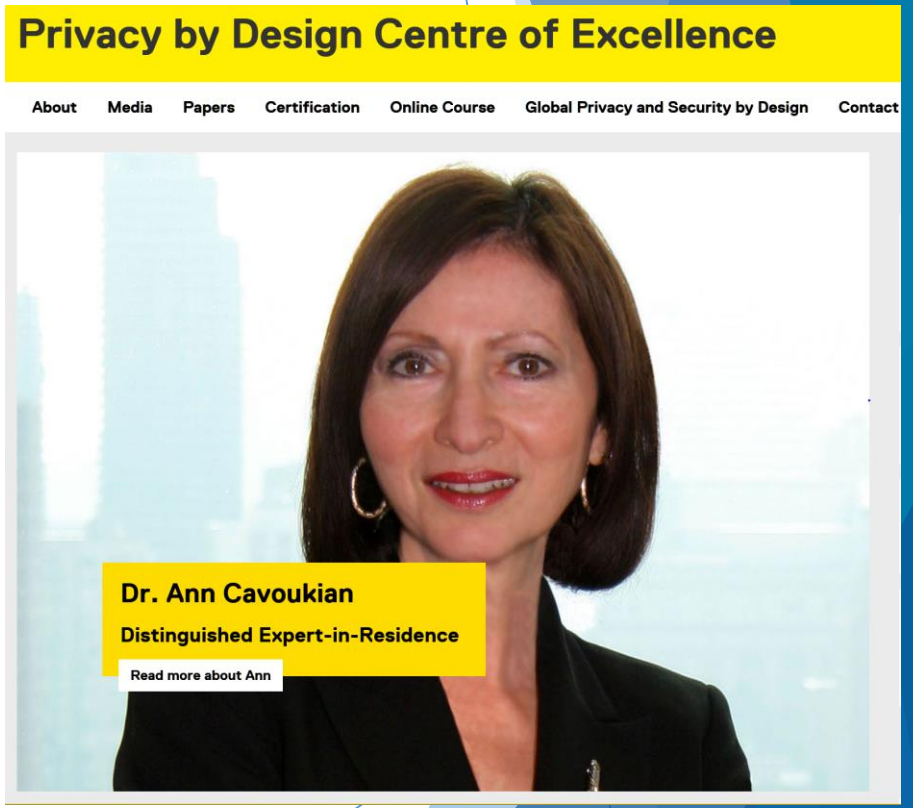
- Company strategy
- Financial data
- Personnel data
- Health data
- Customer data
- Product data
- R&D data
- Partner/vendor data
- Application databases
- Customer history
- Government data
- Other documents
- Spreadsheets
- Presentations
- Photos/diagrams

This is what the bad guys are after...

- Name and aliases
- Social security number
- National identification number
- Driver's license/history data
- Other government identifiers
- Citizenship/legal status
- Gender, race, ethnicity
- Birth date, place of birth
- Home, work and cell numbers
- Personal email address
- Religious preference
- Sexual preference
- Security clearance
- Mailing and home address
- Mother's maiden names
- Spouse information
- Child information
- Emergency contact information
- Biometric data
- Financial/credit card data
- Medical/disability information
- Law enforcement records
- Employment records
- Educational records
- Military records

Introducing Privacy by Design (PbD)

- Seven principles, they assert:
  - Regulatory frameworks are not enough.
  - Must become default mode of operation.
  - Must include both business practices and information systems.
  - It must protect all types of personally identifiable information (PII).



* http://www.ryerson.ca/pbdce/

7 Principles of Privacy by Design

1. **Proactive** not Reactive; **Preventive** not Remedial
2. Privacy as the **Default** Setting
3. Privacy **Embedded** into Design
4. Full Functionality — **Positive-Sum**, not Zero-Sum
5. **End-to-End** — Full Lifecycle Protection
6. Visible and **Transparent** — Keep it Open
7. **User-Centric** — Focus is on respect for User Privacy

P
D
E
P
E
T
U

1. Proactive not Reactive; Preventive not Remedial

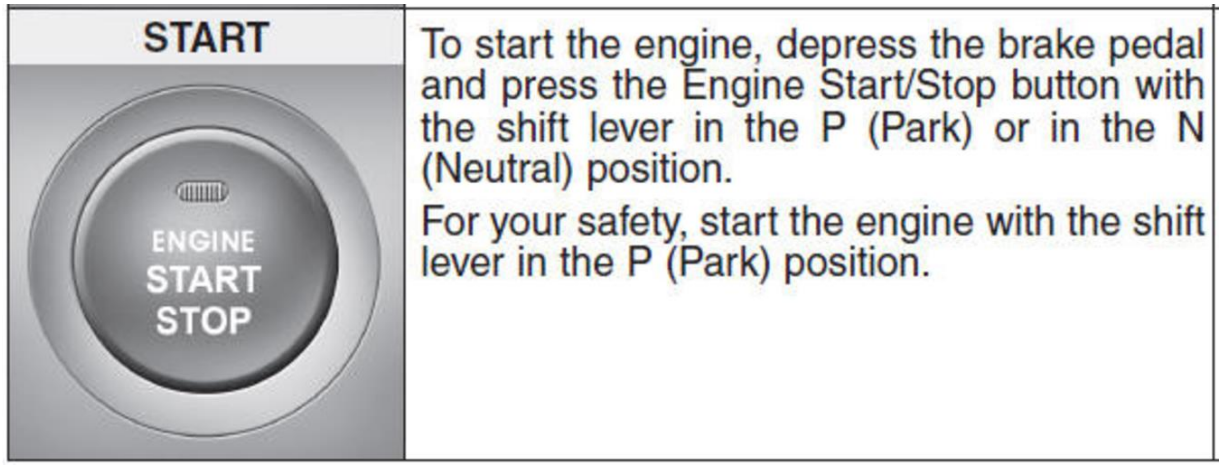
- **Anticipates** and prevents privacy invasive events *before they happen*.
- It does not wait for privacy risks to materialize, it **aims to prevent** them from occurring.
- PbD comes **before-the-fact**, not after.

2. Privacy as the Default Setting

- Helps to ensure personal **data are automatically protected** in any system or business practice.
- If an individual does nothing, their privacy still remains intact.

3. Privacy Embedded into Design

- **Baked into design** of information systems and business practices; not bolted on after the fact.
- PbD becomes an component of the functionality being delivered, **without diminishing that functionality**.



4. Full Functionality; Positive-Sum, not Zero-Sum

- PbD **accommodates all interests** and objectives in a “win-win” manner, not zero-sum approach.
- It avoids the conflict between privacy vs. security, and **works to achieve both**.

5. End-to-End, Full Lifecycle Protection

- Addresses security **before first element of information is collected**.
- Ensures **cradle to grave**, protections throughout information lifecycle, end-to-end.

6. Visibility and Transparency; Keep it Open

- PbD assures **everyone is operating according to the stated (privacy) promises** and objectives.
- PbD component parts, processes and operations remain **visible and transparent** to users and stakeholders.

7. Respect for User Privacy; Keep it User-Centric

- Requires everyone to **keep the interests of individual users the highest priority** by offering:
  - Strong privacy default settings.
  - Appropriate notice about what you hold and how you are using their data
  - User-friendly options for them to control their privacy.

10 ways to use PbD to reduce attack surface

1. Know **what** personal data you are holding.
2. Define and document **why** you are holding it.
3. Reduce, **minimize** what you hold.
4. Rather than holding it use a **data reference** service.
5. If you must hold it, **get permission** from users to hold it and to use it.
6. Where you can, **de-identify** or **anonimize** data.

10 ways to use PbD to reduce attack surface

7. Separate**, partition** data, and under separate authentication.
8. Encrypt **ALL data**, in motion and at rest.
9. Implement **separate** presentation layer security from database security.
10. As soon as you no longer need it, **delete PII**.

BONUS: *Go through these points quarterly, and at the board level.*

For EU: PbD is embedded in the GDPR

- ***GDPR Article 25 Data protection by design and by default***

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Resources to learn more about PBD

- Dr. Cavoukian's PbD Center of Excellence
  http://www.ryerson.ca/pbdce/
- Ryerson University class on PbD
  http://ce-online.ryerson.ca/ce/default.aspx?id=3770
- Ryerson and Deloitte's PbD Certification
  http://www.ryerson.ca/pbdce/certification/
- Hewlett Packard's PbD Toolkit
  http://h41111.www4.hpe.com/privacy-toolkit/overview.html
- Operationalizing PbD
  https://goo.gl/K9udBa


He’s a happier CISO now…
Thanks Chuck!

Thank you

Chuck Georgo

chuck@nowheretohide.org

USA 410-903-6289

NOWHERE TO HIDE.ORG